A large number of business transactions nowadays are being carried out electronically. Electronic transactions are increasing in numbers both in the developed and developing world due to the proliferation of the Internet, mobile devices and electronic services. Individuals and organizations in the developing world are also implementing technologies and legislation for providing, supporting and protecting trade through the Internet and other electronic media.

The Business-to-Consumer (B2C) market via telecommunications services has gained significant attention in developing regions of Africa. The activities and decisions carried out by consumers in-order to purchase goods and services have previously been defined in literature us- ing Consumer Buying Behavior (CBB) models. Traditional structures of e-commerce systems present several limitations for possibilities of service provision in B2C trans-actions. Such systems provide structured catalogs of goods and services with search or navigation facilities through which customers reach their desirable items.

Over the past 10 years, agent systems have been suggested in various operations of electronic commerce (e-commerce) to facilitate automation in CBB models. Industrial practices have demonstrated that more automation is needed on both the suppliers and consumers side to reduce the time and effort required for transactions completion. Automation would also facilitate suppliers to reach target customers faster with customized advertisements, goods, prices and services.

Agent-mediated technologies do not come without challenges. In order for agents to execute tasks assigned to them, they may have to interact with other agents in the environment. Some of these agents or other entities (such as platforms) in the environment could be malicious. These challenges present trust questions among agents and platforms on which they execute. Software agents would typically be required to obtain reputation information from a reliable source in-order to establish the level of trust with which the participating entities should be engaged. Furthermore, reputation models used in agent systems also raise new challenges of strategic liars and informal expectations from participants.

This thesis has developed an agent-mediated system that is secure and incentive compatible based on a double auction market mechanism for agricultural trade in developing countries such as Uganda.

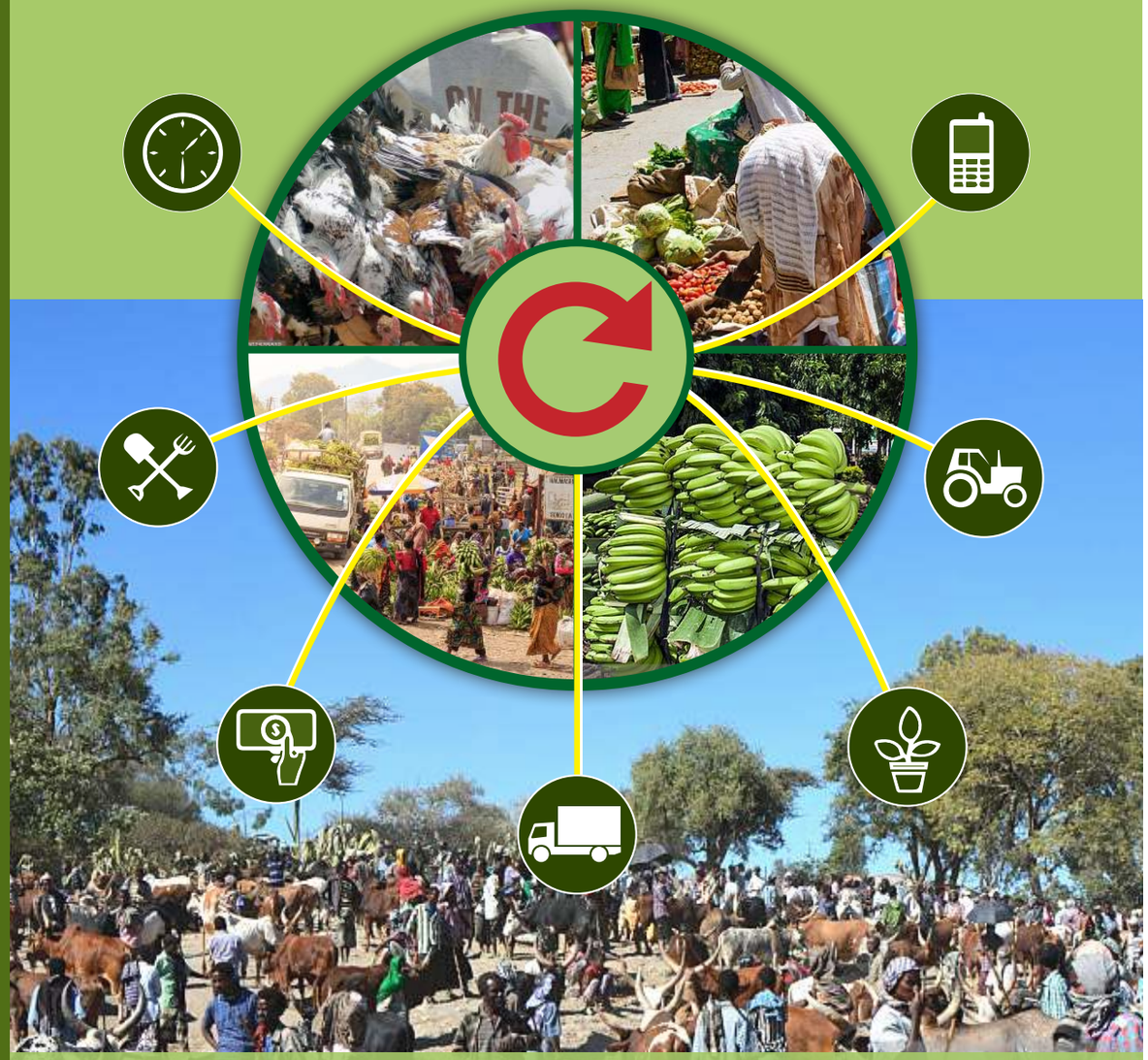
Agricultural markets in developing countries are operated using centuries-old approaches. Despite numerous efforts by various organizations and individuals to develop electronic market systems to support agricultural markets and electronic trade in developing countries such as Uganda, the adoption of these systems has not be realized and many large scale deployments have failed. These failures can be largely attributed to shortcoming in the design of incentive compatible market mechanisms that would encourage buyers and sellers to participate in the market systems.

The solution presented in this thesis is resistant to the security issues mentioned. It is envisaged that this will encourage buyers and sellers to participate in this market system. The system registered 1030 users with commodities worth 2 million US dollars being submitted to the market in a 6 months' pilot study. This enthusiastic adoption of this system suggests that our design has met user expectations.

ISBN 978-94-028-0477-5

Market Design For Agricultural Trade in Developing Countries

Market Design *for* Agricultural Trade in Developing Countries



Richard Ssekibuule

Market Design for Agricultural Trade in Developing Countries

Proefschrift

ter verkrijging van de graad van doctor

aan de Radboud Universiteit Nijmegen

op gezag van de rector magnificus prof. dr. J.H.J.M. van Krieken,

volgens besluit van het college van decanen

in het openbaar te verdedigen op woensdag 11 januari 2017

om 12.30 uur precies

door

Richard Ssekibuule

geboren op 10 april 1979

in Kampala (Oeganda)

Promotor: Prof. dr. ir. Theo P. van der Weide

Copromotor: Dr. John A. Quinn (Makerere University, Kampala, Oeganda)

Manuscriptcommissie:

Prof. dr. H.A Proper

Prof. dr. E.-M. Sent

Prof. dr. H. Akkermans (VU)

Market Design for Agricultural Trade in Developing Countries

Doctoral Thesis

to obtain the degree of doctor
from Radboud University Nijmegen
on the authority of the Rector Magnificus prof. dr. J.H.J.M. van Krieken,
according to the decision of the Council of Deans
to be defended in public on Wednesday, January 11, 2017
at 12.30 hours
by

Richard Ssekibuule
Born on April 10, 1979
in Kampala (Uganda)

Supervisor:
Prof. dr. ir. Theo P. van der Weide

Co-supervisor:
Dr. John A. Quinn (Makerere University, Kampala, Uganda)

Doctoral Thesis Committee:
Prof. dr. H.A Proper
Prof. dr. E.-M. Sent
Prof. dr. H. Akkermans (VU)

Abstract (Dutch)

Een groot aantal zakelijke transacties wordt tegenwoordig elektronisch uitgevoerd, in toenemende aantallen. Dit gebeurt zowel in de ontwikkelde als ontwikkelingslanden, als gevolg van de verspreiding van het internet, mobiele apparaten en elektronische diensten. Ook individuen en organisaties in de derde wereld zijn bezig ook de invoering van technologieën en wetgeving voor het leveren, ondersteunen en beschermen van handel via het internet en andere elektronische media. De Business-to-Consumer (B2C) markt via telecommunicatiediensten heeft veel aandacht gekregen bij de ontwikkeling van Afrikaans regio's. De activiteiten en beslissingen die door de consumenten worden uitgevoerd bij de aankoop van goederen en diensten te kopen uitgevoerd zijn reeds eerder zijn beschreven met behulp van zogenaamde Consumer Buyer Behavior (CBB) modellen. Traditionele structuren van e-commerce systemen leiden tot verscheidene beperkingen voor de mogelijkheden van dienstverlening in de B2C-transacties. Dergelijke systemen bieden gestructureerde catalogi van goederen en diensten met een zoek- of navigatie faciliteiten waarmee klanten de door hen gewenste items kunnen bereiken.

De afgelopen 10 jaar zijn agent-systemen voorgesteld bij diverse bewerkingen van de elektronische handel (e-commerce) om de automatisering van CBB modellen faciliteren. Uit de industriële praktijk is gebleken dat verdergaande automatisering nodig is zowel aan de kant van de leveranciers als van de consumenten om de tijd en moeite te verminderen voor de voltooiing transacties. Automatisering maakt het leveranciers gemakkelijker om de doelgroep van klanten te bereiken met aangepaste advertenties, producten, prijzen en diensten.

Agent-mediated technologieën komen niet zonder uitdagingen. Om de hen toegewezen taken uit te kunnen voeren, moeten agenten wellicht samenwerken met andere agenten uit hun omgeving. Zulke agenten, of andere entiteiten uit de omgeving (zoals het platform waarop ze werken) kunnen kwaadaardig zijn. Dit leidt tot de vertrouwensvraag tussen agenten en de platforms. Een typisch onderdeel is dat software agenten verplicht moeten worden hun reputatie te ontlenen aan een betrouwbare bron, waardoor een niveau van vertrouwen ontstaat dat vereist is voor de betrokken deelnemers. Daarnaast, reputatie-modellen in agent systemen leiden weer tot nieuwe uitdagingen, zoals 'strategic liars' en informele verwachtingen van de deelnemers. In dit proefschrift wordt een agent-mediated systeem ontwikkeld

dat veilig en stimulerend is, gebaseerd op het dubbele veilingsmechanisme voor de handel in landbouwproducten in ontwikkelingslanden zoals Oeganda.

De landbouwmarkt in ontwikkelingslanden werkt vanuit eeuwenoude benaderingen. Ondanks de vele inspanningen van verschillende organisaties en individuen om elektronische marktsystemen voor de landbouwmarkten en elektronische handel in ontwikkelingslanden zoals Oeganda te ontwikkelen, zijn deze systemen niet breed geaccepteerd, en vele grootschalige implementaties zijn mislukt. Deze mislukkingen kunnen grotendeels worden toegeschreven aan tekortkomingen in het ontwerp van stimulerende compatibele marktmechanismen die kopers en verkopers aanmoedigen deel te nemen aan het marktsysteem.

De oplossing voorgesteld in dit proefschrift is bestand tegen de genoemde veiligheidsvraagstukken. Het is de bedoeling dat dit kopers en verkopers zal aanmoedigen deel te nemen aan dit marktsysteem. Gedurende een pilot studie van het het systeem van 6 maanden registreerden zich 1030 gebruikers met goederen ter waarde $2.000.000. Deze enthousiaste adoptie van dit systeem suggereert dat ons ontwerp aan de gebruikersverwachtingen heeft voldaan.

Abstract (English)

A large number of business transactions nowadays are being carried out electronically. Electronic transactions are increasing in numbers both in the developed and developing world due to the proliferation of the Internet, mobile devices and electronic services. Individuals and organizations in the developing world are also implementing technologies and legislation for providing, supporting and protecting trade through the Internet and other electronic media. The Business-to-Consumer (B2C) market via telecommunications services has gained significant attention in developing regions of Africa. The activities and decisions carried out by consumers in-order to purchase goods and services have previously been defined in literature using Consumer Buying Behavior (CBB) models. Traditional structures of e-commerce systems present several limitations for possibilities of service provision in B2C transactions. Such systems provide structured catalogs of goods and services with search or navigation facilities through which customers reach their desirable items.

Over the past 10 years, agent systems have been suggested in various operations of electronic commerce (e-commerce) to facilitate automation in CBB models. Industrial practices have demonstrated that more automation is needed on both the suppliers and consumers side to reduce the time and effort required for transactions completion. Automation would also facilitate suppliers to reach target customers faster with customized advertisements, goods, prices and services.

Agent-mediated technologies do not come without challenges. In order for agents to execute tasks assigned to them, they may have to interact with other agents in the environment. Some of these agents or other entities (such as platforms) in the environment could be malicious. These challenges present trust questions among agents and platforms on which they execute. Software agents would typically be required to obtain reputation information from a reliable source in-order to establish the level of trust with which the participating entities should be engaged. Furthermore, reputation models used in agent systems also raise new challenges of strategic liars and informal expectations from participants.

This thesis has developed an agent-mediated system that is secure and incentive compatible based on a double auction market mechanism for agricultural trade in developing countries such as Uganda.

Agricultural markets in developing countries such as Uganda are operated using centuries-old approaches. Despite numerous efforts by various organizations and individuals to develop electronic market systems to support agricultural markets and electronic trade in developing countries such as Uganda, the adoption of these systems has not be realized and many large scale deployments have failed. These failures can be largely attributed to shortcoming in the design of incentive compatible market mechanisms that would encourage buyers and sellers to participate in the market systems.

The solution presented in this thesis is resistant to the security issues mentioned. It is envisaged that this will encourage buyers and sellers to participate in this market system. The system registered 1030 users with commodities worth 2 million US dollars being submitted to the market in a 6 months' pilot study. This enthusiastic adoption of this system suggests that our design has met user expectations.

Acknowledgement

"A thesis would be incomplete without an acknowledgement page".

This thesis wouldn't have been completed without the unwavering support of Prof. Theo. I am very grateful for the late hours and impromptu meetings you spared to guide me through the process.

I would like to thank Dr. John Quinn for opening the scientific gateways and spending a large part of your time to guide this research work. Several professors have guided me, contributed to this research work and co-authored papers with me. I am very grateful for the kind guidance that I received at the start of my studies from Prof. Erik Poll, Prof. Venansius Baryamureeba, Dr. John Ngubiri and Dr. Jose Quenum. Thanks for all the kind guidance. I would like in-a-special-way to thank Prof. Kevin Leyton-Brown for having made it possible for me to work on the auction mechanism. Thanks for challenging me to always get better with my analytics.

I've studied with many PhD students at both Radboud University and Makerere University. I will take the Ugandan approach of 'political correctness' and not attempt to list your names. I would like to register my sincere gratitude for the camaraderie we shared. The moments we shared in Muzenplaats and 4^{th} floor CIT shall forever be cherished.

I would like to thank NUFFIC — the Dutch fellowship for higher education for providing me with an opportunity to study in a world class University.

Special thanks to my family, my wife Loyce and sons Gregory & Cyrus for patiently waiting and being of great encouragement during the years of my studies.

It was neither by my wisdom nor strength that this thesis was completed — I am eternally thankful for the grace of God for making it all possible.

Contents

1 Research background and approach

This study seeks to address security and automation aspects of agricultural trade systems for developing countries such as Uganda. This chapter presents an introduction to agricultural trade activities in developing countries such as Uganda and presents a background to existing approaches for designing systems for agricultural trade. Section 1.1 presents an introduction to the setup of agricultural markets in developing countries. A background to existing approaches for the design of markets for agricultural trade is presented in section 1.2. In section 1.3, we present a motivation and research problem undertaken for this study. Section 1.4 presents research objectives and questions that we investigated in this thesis. The research approach is presented in section 1.5 and the thesis outline presented in section 1.6.

1.1 Agricultural markets in developing countries such as Uganda

Agricultural markets in developing countries such as Uganda are mostly supported by small scale farmers that grow produce for food and then sell the excess to nearby or roadside markets. The organization of markets in Uganda for example is in such a way that small scale traders and brokers aggregate produce at the farm level and then store it for future sales or sell immediately to traders with large trucks, typically of about 10 tonnes capacity. The large scale traders then transport this produce to urban markets where they sell to wholesale store owners or retailers.

Agricultural markets in developing countries are characterized by high-levels of inefficiency resulting from poor methods of information collection and dissemination [1, 2] between buyers and sellers. Over the past 10 years, the telecommunications infrastructure in developing countries such as Uganda has been developed to meet critical communication needs for both data and voice services. Several information systems have been implemented in form of agricultural advisory services in various developing countries. Gakuru et al. [3] previously presented an inventory of Agricultural advisory services in Sub-Saharan countries.

These advisory services have helped farmers in obtaining information for agricultural best practices to enhance their farm yields. Various implemented electronic advisory services have promised farmers access to market information that they previously did not have. Farmers in developing countries face a problem of competitive pricing for their produce due to an information gap between the markets, traders, brokers and farmers[3]. In 2005, Barrett et al., [1] presented a historical account of various changes and improvements which had taken place in agricultural markets of developing countries since the 1960s.

1.1.1 Current organization of agricultural markets in Uganda

In order for us to gain an understanding of agricultural markets organization in Uganda and similar developing countries, we visited several markets in both the urban and rural areas of the country.

A series of interactions with traders in one popular Ugandan market (Kalerwe) located 4 kilometers from the capital Kampala revealed interesting details about trade organization for agricultural products. Traders learn about products availability through brokers situated in the villages. These brokers are normally acquaintances of the traders with whom they would have exchanged mobile numbers on previous physical interactions. Due to a wide mobile network coverage in the country, brokers do not find difficulty in accessing mobile networks. Proliferation of low-cost mobile phones in the country has also widely eliminated mobile phone accessibility problems. Telephone calling services are also widely available at pay calling stations.

In this environment, brokers play a pivotal role of connecting farmers to traders. The brokers normally get paid depending on the amount and quality of produce that they identify for the traders. When traders perceive goods received through the brokers as being highly profitable, then the broker would get paid more. The negotiations between traders and the brokers are currently informal, with no clear parameters for valuation of broker services. Traders for example purchasing matooke, could make 10 stopovers before obtaining a required load for a 5 tonne truck. If all these stopovers involved a broker, then they would have to pay at each location a fee proportional to the amount of produce collected. For other crops such as potatoes and cassava, the traders could buy the entire garden or a fraction. In such circumstances brokers are paid based on the quality and quantity of the harvest obtained from the garden. Some farmers have organized themselves into small groups for purposes of making bulk sales. This arrangement seems to mostly work well for matooke (bananas) and other products with small yields, but mostly preferred to be purchased in bulk by the traders. Farmer groups have created an improvement in the market organization since small quantities from several farmers can get bulked at shared stores. Bulk

collection points save traders from having to traverse several villages collecting produces in small quantities in-order to obtain the required volumes for a trip.

Our market interactions revealed to us several challenges in the current market organization that we present in the next subsection.

1.1.2 Challenges with the current organization of agricultural markets

Despite improvements in road networks, telecommunication infrastructure and free market conditions in most developing economies, some of the issues that impeded an efficient market place 50 years ago are still prevalent. Agricultural trade in developing countries is still based on informal contracts and market information largely shared by word-of-mouth. Our interactions with the traders revealed that they are always willing to travel to new trade routes or at least recommend them to other traders in neighboring markets. This arrangement seems to have a slow growth rate for trade networks amongst traders and farmers. Discovery of new farmers with desired produce is highly limited to historic interactions with the brokers and farmers. The majority of farmers rely on their small networks of brokers and nearby markets to participate in trade for their produce. Most rural farmers have limited information about market trends for their products and also suffer from small trade networks which essentially reduces their negotiation power for better prices. Traders from urban markets are equally limited to their traditional trade networks which have been known over the years through peers and previous trades. Possibilities of expanding to new trade routes and markets are highly limited due to rudimentary means of learning about trade partners in new and remote locations. Currently, traders communicate with a host of brokers known to them through previous trading activities, but this network does not scale efficiently to create new impact in the market place. The ability for traders to learn about new trade opportunities and for farmers to evaluate demand for their products is limited.

Brokers typically pay informers in the rural areas to alert them about produce opportunities. Brokers and traders also use other methods such as small village billboards in rural areas to advertise their mobile phones to farmers and produce sellers. The presence of brokers in rural markets seems to enhance the market information availability, even though this approach does not scale well for market actors covering an entire country.

Trade networks among farmers and traders hardly grow beyond their historical social networks. Internet based e-commerce systems which have been ubiquitously adopted in the developed have not yet had an impact on agricultural trade in developing

countries. Low bandwidth conditions, poor electricity infrastructure and high entry prices for computers have been significant hindrances to the adoption of Internet supported commerce.

The current market environment suffers from the following major problems;

- The current trading environment requires farmers to collect their produce and wait by the road side for the traders to collect the merchandise. Selling prices for the farmers' products are negotiated on arrival of the traders. These negotiations are typically one-sided, since traders have the leverage of meeting other farmers along their trade routes while farmers have to worry about the long waits and spoilage for their fresh produce.

- In addition to farmers struggling to sell their produce, traders also have to travel long distances with the uncertainty of finding the goods promised to them by the brokers or farmers. This situation arises from the the fact that traders do not have any binding agreements between them and farmers or brokers before they travel to the locations of the merchandise. Typically traders rely on gentleman's agreements established through mobile phone calls and broker contacts. It is also very common for farmers to sell to other traders or brokers that show-up before arrival of those previously negotiated with. Such situations would mean that traders have to travel further along their trade routes or find new ones in order to obtain the required load for their trip. The farmers can afford to act this way due to absence of binding formal trade agreements between stakeholders.

- Farmers usually travel to their trading points with historical price information for their merchandise. It is difficult for farmers to take advantage of changes in market prices since they take long to learn about the changes. Traders normally take advantage of such situations to buy at low prices. Such low cost transactions have a ripple-effect on other activities of the farmers. If the farmers sell at low prices it means that they may not be able to meet costs for drugs and pesticides whose prices might have increased.

1.2 Existing approaches to the design of electronic agricultural markets

Several private and public organizations have contributed to the enterprise support of small scale farmers in Uganda. These efforts have ranged from efforts to increase farm yields, savings and credit schemes, and market linkage growth. Presented in

the enumeration below are systems and organizations which have invested various efforts in promoting dissemination of agricultural market information.

i. **FarmGain:**
FarmGain Africa Ltd (http://farmgainafrica.org) is a firm which specializes in market information for agro-business development. Farmgain has been providing radio and SMS based market information to rural farmers with an alternate web interface for Internet connected users. These prices are obtained from retail and wholesale markets covering Uganda and Kenya. Warid Telecom (www.waridtel.co.ug) has implemented a SIM toolkit application which provides market information reported by FarmGain. This system is pricey for farmers. An SMS for a single commodity costs 150 Ugandan shillings, which is close to the price of a kilogram of maize grain in the rural areas.

ii. **FoodNet:**
Since September 1999, Foodnet (http://www.foodnet.cgiar.org) with support from the International Institute of Tropical Agriculture (IITA) (http://www.iita.org/) has been collecting market information on market data from 19 markets across Uganda. This information was being collected on a daily basis mainly from wholesale markets. Initially this information was disseminated through national newspapers, email, fax, radio stations, government departments and agricultural development agencies.

In November of 2005 an SMS based market information service was launched through MTN and ZAIN telecom operators. Judging by the updates on the website and short number codes (198 and 755) being quoted, it seems that this service is no longer being maintained. Since 2008, mobile phone operators have been required to use 4-digit numbers for provision of SMS based value-added-services.

iii. **FIT Uganda:**
In July of 2008, FIT Uganda (http://www.fituganda.com) a private sector business consulting firm which provides capacity building to SMEs launched an agricultural market information service to provide real-time market information to subscribers. FIT Uganda was funded by Cordaid and DANIDA to implement a market information system to improve access by farmers and traders to affordable agricultural market information.

iv. **AgriNet:**
AgriNet (http://www.agrinetug.net) is a private company in Uganda whose mission is provide agricultural market information to farmers via an SMS interface. The website for AgriNet was last updated in 2008 which is a very

long period for an information service company. Though the information on their website claims goals of market intelligence, this effort has not bared fruits since the market information presented is old and outdated.

v. **GRAMEEN:**
Grameen foundation (http://www.grameenfoundation.org) in partnership with local telecom service provider MTN launched village phones to extend mobile phone services to rural areas of Uganda. These village phones were also used to pioneer initiatives for providing agricultural market information to the rural poor (http://www.grameenfoundation.org/what-we-do/empowering-poor) via group led or call-center units. In 2007, Grameen Foundation started a mobile applications laboratory in Uganda (APPLab (http://www.grameenfoundation.applab.org/section/index)) to promote capacity in the development of software applications aimed at empowering poor communities through ICTs. A two year collaboration with Google and MTN was started to develop a suite of mobile applications to provide market linkage information between buyers and sellers. A mobile based service known as Google Trader (http://www.google.co.ug/africa) was thus launched in 2009 as a result of this collaboration. Google Trader provided a listing of general merchandise (Agriculture, appliances, housing, etc) with their price information, location and contacts through web and SMS interfaces. In addition to this service providing only classifieds of items available for sale, only MTN subscribers can use it. This exclusivity might be linked to the longterm partnership between MTN, Google and Grameen.

vi. **NOGAMU:**
National Organic Agricultural Movement of Uganda (NOGAMU) (http://nogamu.org.ug) has particularly been focusing on linking farmers to reliable buyers. NOGAMU's market information services have focused on organic export opportunities for local farmers. An organic trading point (OTP) containing profiles of target international markets was created to advise existing and potential exporters. This information resource is not readily available to small scale rural farmers since it can only be obtained either by email requests or physical visits to the NOGAMU offices.

International market linkage efforts by NOGAMU present an important possibility for rural farmers being organized into sub-county/regional groups which could be motivated to produce more organic products for export.

vii. **NAADS:**
Most of the work related to the mobile-phone-based market have only been concerned with market information dissemination component. According to

	Farmgain	Foodnet	FIT Uganda	AgriNet	Google Trader	NOGAMU	NAADS	Proposed system
Link buyers to sellers	Y	Y	Y	Y	Y	Y	Y	Y
Dynamic Integration of Pricing	N	N	N	N	Y	Y	N	Y
Information type collected	P	P, V	P	P	P	P,V		P,V,Q
Price info	Y	Y	Y	Y	Y	Y	Y	Y
SMS Support	Y	Y	Y	Y	Y	Y	Y	Y
Trade Support	N	N	N	N	Y	Y	N	Y
Support Group Marketing	N	N	N	N	N	N	Y	
Support Agric Training	N	Y	N	Y	N	N	Y	
Update Frequency	X	W		X	D	X	X	D

Legend:
Y=Yes, N=No, P=Price, V=Volume, Q=Quality, D=Daily, W=Weekly, X=Not Applicable

Tab. 1.1.: *Agricultural Market Systems Comparison*

farmer groups information obtained from the National Agricultural Advisory Services (NAADS)report of 2003[4] [1] indicates that 8,638 groups were formed between 2002 and 2003 in the 16 participating districts. Currently, Uganda has a total of 111 districts. These groups were represented by heads tasked with disseminating information amongst their members through short messaging services (SMS) and voice mobile calls.

This review also shows that the analyzed systems mostly provide classified of items available for sale, but do not facilitate trade. A part from stating that you can buy item X from person Z, it is not possible to know whether the item was actually bought and neither is it possible to know the prices and negotiations involved. This essentially makes it difficult to have active updates for market information due to dependency on data collectors. A system through which this information can be gathered from actual tradings would provide more accurate and reliable information. Furthermore, the costs of obtaining this data would be significantly lower, since data collectors do not need to be paid to visit markets to collect prices information.

[1] This is the most recent report from NAADS on groups facts and figures

Figure 1.1 presents a comparison table for features of the reviewed systems against those in the proposed mobile-phone based market system.

1.3 Motivation and research problem

Agricultural market interactions between farmers and traders in the current trading environment has been greatly improved by the introduction of mobile phones and the wide coverage of the GSM network in the country. However, this communication has changed very little of the procedures and techniques for actuating transactions between farmers and traders. Traders still rely on word-of-mouth for discovery of new farmer locations and farmers still rely on informal links with a loosely connected network of brokers to sell their merchandise.

It has been more than 20 years since the creation of successful electronic commerce systems such as Amazon (`www.amazon.com`) and EBay (`www.ebay.com`). Despite the rapid growth of e-commerce systems, their usage and adoption in the developing countries is still very low. Such slow growth might be attributed to several limitations such as power infrastructure, lack of computers, sparse Internet connectivity and absence of credit or debit card systems. This situation has not be different for Uganda. Internet access is still pricey and out of reach for low income earners that form a majority of the population in agricultural trade.

The growth of mobile networks and low cost mobile phones in Uganda has been very fast over the past 5 years. Uganda has a wide GSM network coverage with over 9.4 million people (31% of the total population)[2] having access to a mobile phone [5]. Given this proliferation of mobile phones, it is envisaged that a mobile-phone based market system would improve market information exchange for agricultural trade in a manner similar to e-commerce systems in the developed countries.

The current market environment gives high negotiation power to the traders since farmers have to travel and wait by road side markets with risks of spoilage for their produce. The mobile-phone-based market systems is expected to alleviate this problem by facilitating farmers to interact with several traders and brokers via their mobile phones before traveling to the markets. Better still, these negotiations could be carried out before harvesting to further alleviate worries of spoilage for farmers' produce. A mobile-phone-based market system is expected to offer farmers a gateway to market information so that they can price their products more competitively.

The mobile-phone-based market system is expected to offer traders and farmers a formal procedure through which agreements can be created between parties

[2] Uganda has a young population, with 49.9% of the population below the age of 14 [5].

engaging in various trade activities. The proposed auction system is expected to provide evidence for agreements entered into by various trading partners. The negotiation interactions between stakeholders would provide concrete information for creation of formal agreements between farmers, brokers and traders. Payments through a mobile-money services could also act as commitment from either party to the transaction agreement. Traders would have greater ability to plan and optimize their trade routes since the trade expectations would have been defined before starting their trip.

In the current environment, brokers act as market facilitators since they are typically more informed about the market than farmers and more informed about rural areas than traders. The participation of brokers in the current agricultural trade environment is considered to be highly disadvantageous to farmers. Brokers typically make very high profit margins while farmers barely break even.

As previously indicated by Jensen et al., [6] brokers play a key role in supporting market transactions and should not be eliminated despite the involved costs. The mobile-based market system is expected to provide brokers with new transparent roles to more effectively improve the overall effectiveness of the agricultural market system. The new role played by brokers is expected to be more transparent to both the traders and farmers since all groups would have access to market information and pricing details for various markets in the country.

1.3.1 Shortcomings of price advisory systems

Price advisory systems are ineffective for several reasons. First, there can be problems with data accuracy and relevance. Information is gathered by asking buyers and sellers to report the current price for different products. However, both parties are biased, and reported prices may therefore fail to accurately reflect actual sales taking place. Even when price estimates do accurately reflect actual sales in one place, they often fail to reflect prices for individuals of different circumstances across a wider region. For example, a farmer selling goods who is located a long way down a bad road will be able to sell good at a lower price than a farmer conveniently located next to a highway. In addition, only mean prices are reported, giving no indication of supply and demand curves. Price information is therefore unhelpful to farmers who are very eager to sell even at a low price, or farmers who have less need to sell and are prepared to wait for a high price.

The structure of most advisory services also fails to provide detail about produce specifications. For example, we found that all price information provided by FEWS-NET does not contain species information. This is important because prices can vary by 20% between different species of crops such as beans, potatoes, coffee and rice.

1.3.2 Shortcomings of classified listings and single-sided auctions

Classified listings, in which sellers and buyers post descriptions and offered prices, are problematic when the mode of communication is SMS on a simple phone (with a small screen), because the medium makes it impractical to view the details of more than one or two items. Single-sided auction markets, in which buyers view and bid on individual items, have the same problem, and indeed may require even more communication to complete a trade. Such markets are not well suited to commodity trading, as they do not take into account the fact that commodities are inherently exchangeable and thus not every potential match needs to be viewed by a buyer or seller.

An auction market system known as "Robit" was proposed by Reda et al. [7] for use in settings where communication channels are narrow and possibly expensive, through the use of SMS and telephony voice kiosks. Robit makes use of a second price auction design mechanism for commodity trading. The implementation also makes use of a communication platform called Sulula [8] which provides a reliable connectivity with caching for individuals in constrained environments. While this work is interesting and useful to the research community, we have three main concerns about its practicality. First, the proposed scheme is silent about what happens when a buyer or seller has more than one match for their bid or ask; we assume that the user will be presented with possible matches one at a time following a right-of-first-refusal protocol. This means that users need to look through a list of matches for bids or asks. This is likely to be problematic for users with 'feature-phones' that have limited space for display. Second, another problem is SMS costs. Market participants would bear higher costs with the greater amount of traffic required by this system; furthermore, it would also be unsustainable for the system operator, which would be required to send a large amount of acknowledgment and notification messages. Third, Robit addresses the information asymmetry problem by providing voice product descriptions. While these descriptions may be more engaging for participants, we worry that they would do little to discourage dishonest product descriptions.

1.3.3 Shortcomings of existing multiparty computation solutions

In Bogetoft et al. [9] a multiparty computation solution that aims to provide a fair distribution of resources while preserving privacy of participants is presented. The article proposes utilization of double auction mechanism to derive a *market clearing* price which is found at the intersection between demand and supply of the commodities being traded. We can observe a flaw or weakness with determination of the clearing price (quoted as MCP).

When the clearing price is left to the potential prices of bids and asks, you get problems fixious bids and asks being submitted in the market to influence the outcome of an aution. In this scheme buyers and sellers do not need to bid and ask truthfully. Pseudo bid and ask prices can artificially inflate demand and therefore a wrong clearing price would be set.

This paper largely focused on cryptography and privacy preservation but failed on robustness of the auction mechanism. The auction mechanism that we designed presents unique solutions for a unique market in Uganda and similar developing countries; where by techniques that are feasible with web and smart-phone systems are not achievable with feature-phones. In the pilot that we carried out in 4 districts of Uganda, we hardly came across more than 1 in 100 farmers with smart phones. The entire region we surveyed did not have access to internet facilities.

1.4 Research questions and objectives

As presented in section 1.2, we see documented effort to develop system to improve agricultural trade in developing countries such as Uganda. These systems however have shortcoming that we have presented in section 1.3 and therefore fail to meet trader and farmer needs. The absence of electronic system has maintained an environment that operates on centuries old approaches. We argue that these approaches are inefficient and do not facilitate sufficient trade traffic.

The main objective of our research work is to develop a system that has the right incentives for farmers and traders to actively participate in the market. In doing so, we anticipate to make a positive contribution to the improvement of agricultural trade.

Consequently the key research question that this research aims to address is;

"*How can we design systems that enhance agricultural trade in developing countries such as Uganda?*"

In order to answer this overall question, this research will address the following specific research questions;

i. What are the key characteristics of an inefficient market for agricultural trade in developing countries?

ii. What are the key factors that contribute to agricultural trade inefficiency and how can we address them?

iii. What are the key trust and security concerns in the current market environment and how do we plan to address them?

iv. What are the key parameters for evaluating an improved system for agricultural trade in developing countries?

1.4.1 General objective

In order for this research work to address the general and specific research questions in subsection 1.4 above, this thesis aims to achieve the objectives that are presented here.

The general objective of this research work is to contribute towards techniques necessary for developing secure and incentive compatible electronic-markets in developing countries.

A design mechanism is said to be *incentive compatible* or *truthful* if at all times a $player_i$ can find a strategy θ_i that is dominant (optimal) no matter what the other players do [10].

1.4.2 Specific objectives

The specific objectives for this research project are thus derived from the general objective and security challenges presented in section 3.1.3. In order to achieve the general objective, the specific objectives of the research are:

i. to design an incentive compatible auction market for mobile-based agricultural trade in developing countries such as Uganda.

ii. to develop extended threat models for agent-mediated applications in an open-distributed environment.

iii. to design and implement an agent-mediated auction market for autonomic trading based in an open distributed environment.

iv. to test and validate the designed and implemented applications based on the defined incentive compatibility and security requirements.

1.5 The research approach

Undertaking a research effort to improve agricultural markets in developing countries such as Uganda is a largely multi-disciplinary effort. This research is multi-disciplinary in the sense that it requires an understanding of the following areas of research;

i. An economics point of view for defining market efficiency and attributes of an inefficient market.

ii. An economics and mechanism design (Game theory) understanding and interpretation of causes for inefficiencies in the agricultural market environment.

iii. An information scientific evaluation of existing solutions and attempts to solve the information asymmetry problem among market participants.

iv. From a computer science and design science perspective, we investigate new and existing technologies or techniques that could be used to deliver a solution that meets our research goals.

The research approach defines the underlying philosophies, methodologies and strategies that were used to derive the research problem [11]. This perspective is used to create a foundation for designing and implementing a platform that aims to improve agricultural market in developing countries such as Uganda.

The subsections that follow present details of the research strategies that we used in this study.

Agent systems study and prototyping

We reviewed a significant amount of literature presented in section 3.2 on automation using an agent-systems approach. In order to put the literature reviewed into context, we implemented a prototype agent-mediated application on two types of agent middleware. A detail description of this implementation is presented in the appendix A. This agent-mediated prototype was used to model threats for such applications. We also used the agent-mediated prototype to review security and automation requirements for generic application implementations. The automated book-trading application was used to study underlying platform security requirements and implementation artifacts for agent-mediated automation. — this was aimed to contribute to techniques for automation and security in electronic trade.

Analysis of agricultural market efficiency

In the context of agricultural trade, we carried out an evaluation of agricultural markets efficiency for developing countries 2.4 and analyzed historical market data collected by FEWSNET [12] for Ugandan wholesale markets. We analyzed historical market data for presence of temporal and spatial arbitrage opportunities. The agricultural markets information analysis provided us with a tremendous insight into agricultural markets configurations in Uganda and helped us study patterns of arbitrage in the country. It was highly evident in the results that Ugandan agricultural markets exhibit elevated levels of inefficiency due to temporal and spatial arbitrage opportunities that we discovered.

After obtaining results for the market analysis, we embarked on investigating factors that led to such high-levels of inefficiency. We evaluated existing systems of trade in Uganda — this spectrum also included traditional word-of-mouth trade linkages and other forms of electronic trade via mobile phones and the Internet 2.3. We again observed that many designs of these systems were not incentive compatible with buyer and seller requirements.

Prototyping of an electronic market for agricultural trade

Before we embarked on designing a new market system, we visited over 5 agricultural markets around Kampala to interact with traders — in-order to understand the details of their operations. These interactions gave us a renewed understanding of challenges faced by traders and farmers from the traders' perspective. We also visiting 4 farming districts in central Uganda to in order to understand and appreciate farmer approaches to agricultural trade. We obtained a new and detailed understanding of agricultural trade from the farmers' perspective and traders' perspective. After these interactions, we could appreciate why previous market designs we not well suited for the market environment in developing countries such as Uganda.

Farmers in agricultural countries similar to Uganda have fuzzy measurements for quality even for global products such as coffee. We observed that our market designs were supposed to cater for such peculiar interactions between traders and farmers. The results of these interactions guided our efforts to pursue a market design that is incentive compatible and robust against security threats in an open distributed environment.

Testing and piloting of our market designs and implementations

The design our market mechanism also went through a testing approach. We had several design concepts that looked concrete on paper but impractical for farmers and traders. These market considerations are presented in the appendix section 5.2. We piloted the market system through interactive meetings with traders in Ugandan city centers and farmers in both urban and rural areas. The interactive design approach which follows an Agile methodology [13, 14] for software developed helped us combine scientific methods for software design with a rich understanding of agricultural methods to obtain an incentive compatible market system.

Our study of agent-systems and prototyping with Agentscape and Jade, provided us with a strong software development methodology which aided in development of a software system is robust and secure in an open distributed environment. The implementation of the market design interfaces with 3 telecommunications companies in Uganda and is hosted on a cloud server with universal accessibility to the entire world through the Internet. This platform has been online for more than 3 years with a security incident or application bleach from the Internet. This level of robustness and stability of the market system is attributed to an implementation model which follows an agent-mediated model and grounded approached to software development.

1.6 Thesis organization

The rest of the thesis is organized as follows;

Chapter 2: A Case study of agricultural trade in Uganda

In this chapter we formulate the general problem that is being addressed throughout our work. We present an analysis of agricultural markets in Uganda (as a developing country) and evaluate the status of market efficiency for agricultural produce. The analysis draws parallels with other developing countries whose market configuration bares similarities with that of Uganda. Historical market data from Ugandan wholesale markets is analyzed to determine the extent of temporal and spatial arbitrage opportunities available.

This chapter is based on the article "A Mobile Market for Agricultural Trade in Uganda", *Proceedings of the 4th Annual Symposium on Computing for Development*, 2013 by the author, John Quinn and Kevin Leyton-Brown.

Chapters 3 and 4: The underlying techniques for automated and privacy preserving auction mechanism

These chapters presents underlying techniques that are key to provisioning of automation and secure interactions in agricultural electronic markets. We present an analysis of security implications for various settings of agent-mediated negotiation frameworks and present security implications for three example design configurations. We present an overview of unique threats faced by negotiation frameworks, discuss implications of the threats and possible countermeasures. The chapter also presents confidentiality, privacy and integrity requirements for Publishers and Subscribers in a Publish-Subscribe mediated electronic market. A conceptual market for publishers (sellers) and subscribers (buyers) is presented to to offer an abstract evaluation of security requirements for a virtual-market environment. We review techniques previously suggested in literature for providing confidentiality, privacy and integrity requirements and then present a new solution which is based on cryptographic hashes and public-key cryptography. We present an introduction to publish-subscribe systems, their relationship to the consumer buying behavior model and security requirements for their deployment in a multi-agent environment.

This chapter is based on the articles; "Security in Agent-Mediated Negotiation Frameworks", *In Proceedings of the Twentieth European Meeting on Cybernetics and Systems Research*, 2010, "Mobile-Agent Security Against Malicious Platforms," *In Cybernetics and Systems An International Journal*, vol. 41, no. 07, 2010 and "Secure Publish-Subscribe Mediated Virtual Organizations", *In the Ninth Information Security South Africa*, 2010 by the author.

Chapter 5: An auction system for improved agricultural trade in developing countries

This chapter presents the need for developing an incentive compatible electronic market that efficiently connects trader agents in search of farmer agents with produce for sale and farmer agents in search of trader agents in need of produce to buy. To this end, this chapter presents an auction market for agricultural trade that operates using a Short Messaging Service (SMS) interface. We consider constraints for technology deployment in developing-world agricultural markets and conclude that neither of the existing approaches is sufficient. We argue instead for the introduction of a novel market mechanism better adapted to these constraints—particularly, to the need for interacting with the market via a basic (non-Internet-enabled) phone.

This chapter is based on the article "A Mobile Market for Agricultural Trade in Uganda", *Proceedings of the 4th Annual Symposium on Computing for Development*, 2013 by the author, John Quinn and Kevin Leyton-Brown.

Chapter 6: Evaluation of an incentive compatible auction system for agricultural trade

This chapter presents experimental and evaluation results for the auction market which was implemented based on the principles of agent-mediated frameworks in a Consumer Buying Behavior model. We present a discussion of the design decisions we under took for the auction system and reputation mechanism to maintain an incentive compatible market for agricultural produce. In this chapter we further discuss the initially proposed auction interaction protocols and assumptions for the market environment. We also present outcomes for the field trials that we conducted through field visits and radio advertising.

This chapter is based on the article "A Mobile Market for Agricultural Trade in Uganda", *Proceedings of the 4th Annual Symposium on Computing for Development*, 2013 by the author, John Quinn and Kevin Leyton-Brown.

Chapter 7: Conclusions from the research

This chapter presents our conclusions and evaluations from the research study with the perspective of reflecting on the research objectives and questions. We present our views on limitations of some approaches we used in the study and also evaluate the challenges faced. This chapter ends with conclusions from the study and an outlook of future research activities to be pursued.

2 Analysis of agricultural trade efficiency in Uganda

This chapter presents an analysis of agricultural markets in Uganda (as a developing country) and evaluates the status of market efficiency for agricultural produce. The analysis draws parallels with other developing countries whose market configuration bares similarities with that of Uganda. Historical market data from Ugandan whole-sale markets was analyzed for presence of temporal and spatial arbitrage opportunities. Traders and farmers in urban and rural markets were interviewed to gain understanding of their market environment. The qualitative and quantitative findings are in agreement that agricultural markets in Uganda are largely inefficient despite various efforts to develop market information systems to facilitate agricultural trade in the country. Section 2.1 presents an introduction to agricultural markets in Uganda and presents close comparisons with markets in other Sub-Saharan countries. In section 2.2 we present a multi-agent model for farmer, broker and trader agents in the Ugandan agricultural trade. Section 2.3 presents utility models for multi-agent actors in agricultural markets. In section 2.4 we perform a quantitative evaluation of the Ugandan agricultural market efficiency. Section 2.5 presents an analysis summary of our study and conclusions.

2.1 Introduction

Agricultural production in Uganda is largely supported by small scale farmers that cultivate their crops in predominantly two rainy seasons of the year. Food crops such as bananas, cassava, potatoes, vegetables and cereals are grown by small scale farmers for both their home consumption and commercial purposes [15]. Farmers in rural areas typically receive small revenues from their produce partly due to limited market access and information. Rural farmers typically depend on roadside pick-ups by merchants from urban markets in-order to sell their produce.

Agriculture forms the backbone for the Ugandan economy. As of the year 2013, 87% of the Ugandan population lived in the rural areas [5] mostly depending on subsistence and small scale commercial farming. Traders and farmers struggle to find each other in this environment. Traders for example purchasing cooking bananas,

could make 10 stopovers before obtaining a required load for a 5 tonne truck. If all these stopovers involved a broker, then they would have to pay at each location a fee proportional to the amount of produce collected. For other crops such as potatoes and cassava, the traders sometimes negotiate to buy an entire garden or a fraction. The price for such transactions depends on anticipated quality and quantify of the harvest and market prices for the produce. In such circumstances brokers are also paid based on the anticipated outcome of the harvest, which is usually a fraction (between 5% to 10%) of the buyer's purchase price.

This research work presents our investigations into operations for agricultural markets in developing countries. The following section in the chapter present a background for activities and procedures that farmers undertake to find buyers and means through which traders find farmers for produce to buy. In this study, we use Uganda as a case study for an in-depth understanding of market structures in developing countries. Uganda is located in the eastern part of Africa and tends to have most of the characteristics found in developing countries [5] most especially in the sub-Saharan Africa.

2.2 Market Environment for Farmer, Broker and Trader Agents

To gain further insight into the current operation of agricultural trade in Uganda, we interviewed farmer and trader agents in and around Kampala to learn and understand better their market experiences. Specifically, we met with five traders and seven farmers dealing in maize, beans, groundnuts and coffee. We were particularly interested in the trading process between wholesale dealers in Kampala and producers in the countryside.

Overall, we learned that wholesale dealers commission trucks to pick up produce, and vary in the rural locations they are willing to travel to in order to find seller agents. We found that communication between farmer and trader agents in the current trading environment has been greatly improved in recent years by the introduction of mobile phones and the wide coverage of the GSM network in the country. However, this communication has had little impact on the ways that farmer and trader agents actually find each other and conduct transactions. In particular, trader agents still rely on word of mouth for discovery of new farmers, and farmer agents still rely on informal links with a loosely connected network of broker agents to sell their merchandise. More specifically, we found that:

- The current trading environment has a high opportunity cost for both seller and buyer agents. Farmers harvest their produce and wait by the roadside for

traders to collect their merchandise, risking spoilage if there are no buyers. Similarly, trader agents bringing trucks from an urban market have to devote resources in traveling to areas in which they hope to buy produce without being sure of what they will find.

- Prices for farmers' produce are negotiated when trader agents arrive. Trader agents incur higher transaction costs in finding trading partners, but also tend to have a stronger bargaining position because they have a greater number of options in their trading partners and access to better price information. Farmers with fresh produce can be forced to sell at a low price when faced with potential spoilage if no agreement is reached.

- Farmer agents take longer to learn about changes in supply and demand than trader agents. The profits resulting from short term spikes in urban wholesale prices therefore tend to be taken by traders.

- Trader agents can face considerable uncertainty in finding the goods they are looking for. Local broker agents in rural locations advise trader agents about farms with produce ready to sell, but trader agents currently find this process to be unreliable. Traders may try to get a seller to agree to reserve their produce (though without settling on a price, as mentioned above), relying on gentleman's agreements established through mobile phone calls and broker contacts. Despite entering into such agreements, farmers may still sell to trader or broker agents that show up first.

2.2.1 Experiences with Farmers

The majority of farmers rely on their small networks of broker agents and nearby markets to participate in trade for their produce. Most rural farmer agents have limited information about market trends for their products and also suffer from small trade networks which essentially reduces their negotiation power for better prices. Trader agents from urban markets are equally limited to their traditional trade networks which have been known over the years through peers and previous trades. Possibilities of expanding to new trade routes and markets are highly limited due to rudimentary means of learning about trade partners in new and remote locations. Currently, trader agents communicate with a host of broker agents known to them through previous trading activities, but this network does not scale efficiently to create new impact in the market place. The ability for trader agents to learn about new trade opportunities and for farmer agents to evaluate demand for their products is limited.

Some farmers have organized themselves into small groups for purposes of making bulk sales. This arrangement seems to mostly work well for matooke (cooking bananas) and other products with small yields, but mostly preferred to be purchased in bulk by the traders. The farmer groups have created an improvement in efficiency of the trading environment. Bulk collection points save traders from having to traverse several villages collecting produces in small quantities in order to obtain the required volumes for a trip.

2.2.2 Experiences with Traders

An interview with traders in one popular Ugandan market (Kalerwe) located 4 kilometers from the capital Kampala revealed interesting details about trade organization for agricultural products. Trader agents learn about products availability through broker agents situated in villages. These brokers are usually acquaintances of the traders with whom they would have exchanged mobile numbers on previous physical interactions. Due to a wide mobile network coverage in the country, brokers do not find difficulty in accessing mobile networks. Proliferation of low-cost mobile phones in the country has also widely eliminated mobile phone accessibility problems. Telephone calling services are also widely available at pay calling stations.

Our interactions with trader agents revealed that they are always willing to travel to new trade routes or at least recommend them to other traders in neighboring markets. This arrangement seems to have a slow growth rate for trade networks among traders and farmers. Discovery of new farmers with desired produce is highly limited to historic interactions with the brokers and farmers.

2.3 The Existing Multi-Agent Market Model

This section presents a multi-agent model for the current agricultural market environment in Uganda. We discuss the utility models for farmer, broker and trader agents in the market and discuss how this relates to market efficiency. We represent the broker, farmer and trader environment using a multi-agent paradigm of interaction which is shown in figure 2.1. This model represents and environment in which agents of similar or different types (farmers, traders and brokers) can directly interact with each other in the same locality or communicate across localities via an established communication channel. The Foundation for Intelligent Physical Agents (FIPA) [16] further defines an interaction protocol for request-response interaction which is show in figure 2.2. The consumer in this model makes a request to suppliers and a supplier in-turn makes a response to the consumer. The consumer would then either accept and confirm or reject the response from the supplier.

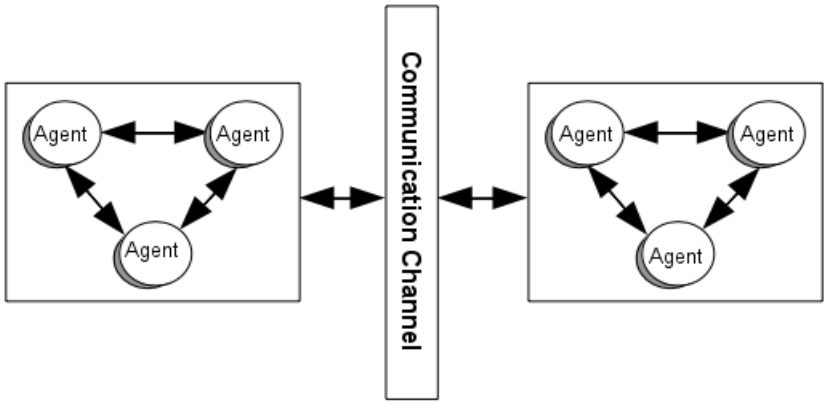


Fig. 2.1.: *Agent-based organization for farmer, broker and trader agents*

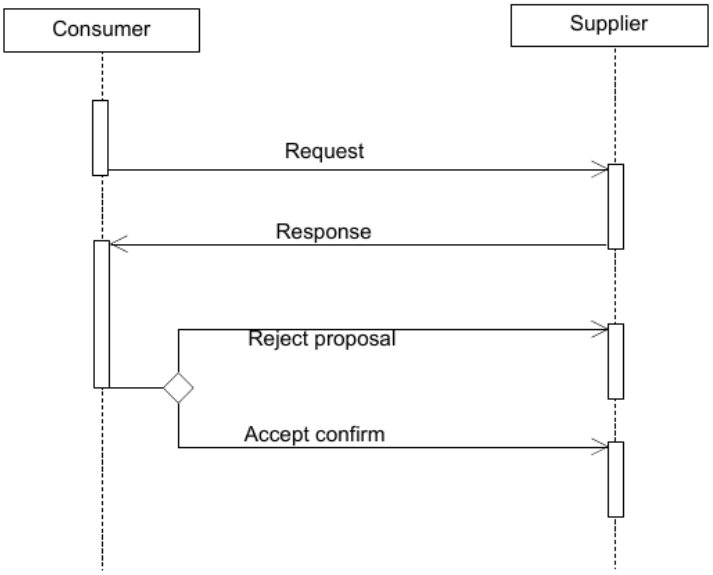


Fig. 2.2.: *FIPA-Based Demand-Supply Agent Model*

The current market environment in the Ugandan agricultural market involves brokers buying produce from farmers and selling it to wholesale and retail traders in urban and semi-urban markets. In this environment, brokers play a pivotal role of connecting farmers to traders. The brokers normally get paid depending on the amount and quality of produce that they identify for the traders. When traders' perceive goods received through the brokers as being highly profitable, then the broker would get paid more. The negotiations between trader and broker agents are thus based on costs incurred by brokers (C_b) to obtain and transport produce to wholesale or retail markets. On the other hand traders valuations for broker services are priced based on the trader-utility (μ_T) anticipated the market. The traders, brokers and farmers agent model is presented using tuples $\mathcal{Q} = (\mu, \mathcal{C}, \mathcal{P})$ which consist of the agents' utility μ, the cost incurred to perform a given task such as

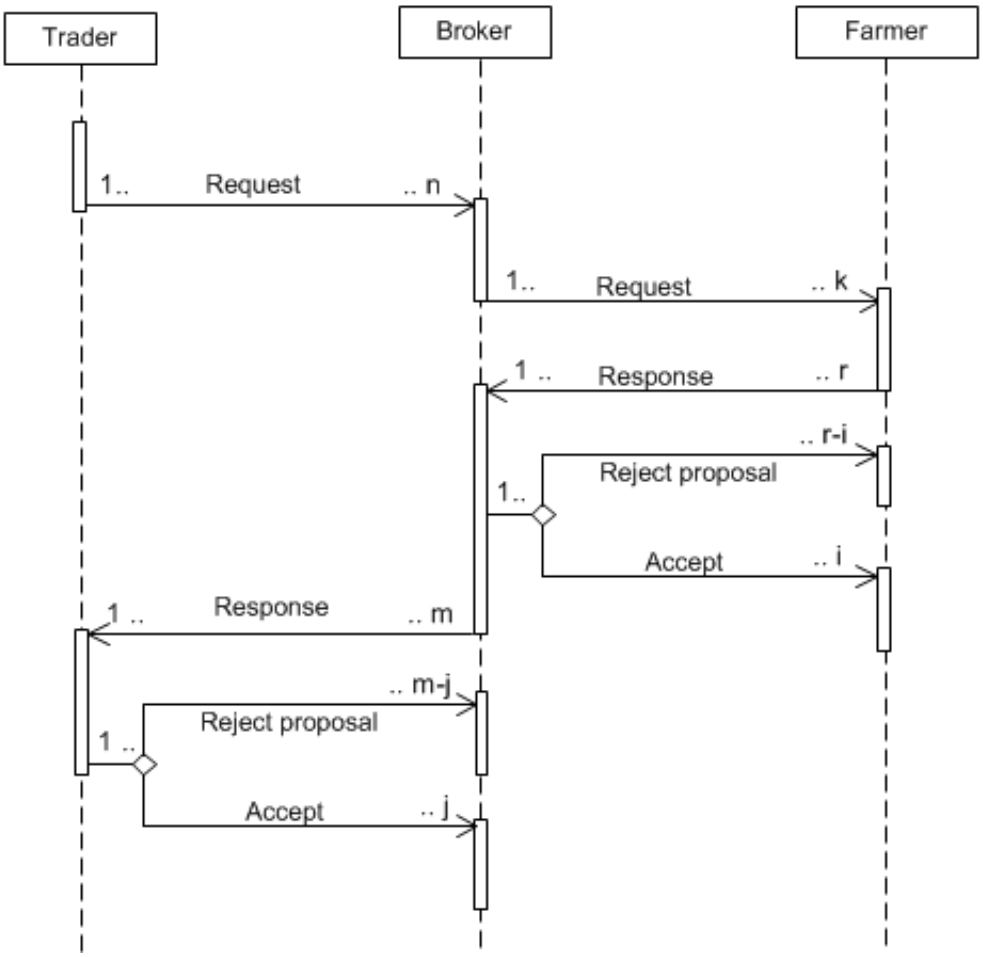


Fig. 2.3.: *FIPA-Based broker, farmer and trader Agent Interaction Model*

growing produce or searching for produce as $\mathcal{C}$ and the price for a given commodity as $\mathcal{P}$.

- The farmer agent utility (μ_F) is computed as $\mathcal{P}_\mathcal{F} - \mathcal{C}_\mathcal{F}$ where C_F is the cost incurred by the farmer agent to put the produce onto the market and P_F is the selling price of the produce.

- The broker agent utility (μ_B) is computed as $\mathcal{P}_\mathcal{B} - (\mathcal{P}_\mathcal{F} + \mathcal{C}_\mathcal{B})$ where $\mathcal{C}_\mathcal{B}$ is the cost incurred by the broker in finding produce and bringing it to the market.

- The trader agent utility (μ_T) is computed as $\mathcal{P}_\mathcal{T} - (\mathcal{P}_\mathcal{B} + \mathcal{C}_\mathcal{T})$ where $\mathcal{C}_\mathcal{T}$ represents the costs incurred by the trader to obtain produce from the broker without the purchase price.

The interaction between these three agents is represented in an agent interaction model which is shown in figure 2.3. In this figure the initial request comes in from a trader agent that contacts brokers (n) for a desired commodity. The broker agents in

turn contact a network of farmer agents (k) for the commodity requested by a trader. A number r out of the k number of farmers contacted by the broker, are considered to have made offers to the broker. The broker filters through the submitted responses (r) from farmer agents — rejecting those that do not meet the required specification and accepting those that are considered acceptable to the trader agent. The broker in this example model is considered to have accepted offers from i number of farmers and rejected $(r - i)$ number of offers from farmers. The broker agents then also submit responses to the trader agent based on what was received from farmer agents. This model considers that a number m of brokers out of n that received the request from the trader responded. The trader agent then accepted a j number of offers from brokers and rejected $(m - j)$.

We argue that the current market organization is highly inefficient. Almost all market agents have to independently evaluate submissions from there counterparts. Firstly, the trader has to keep memory of a collection of brokers that would possibly get him good deals. He has to look around for n brokers and then submit requests to them. The brokers on the other hand also have to reckon with the cost of contacting sparsely located farmers and identifying the most reliable among them to be requested for produce quotations. The broker also has to perform evaluations for all the response received (r) from farmers and select the most optimal to be submitted to the trader. The trader also has to perform memorizations and evaluations similar to those of brokers with all requests sent and responses received.

2.4 Quantitative Evaluation of Market Efficiency

In this section, we perform a quantitative evaluation of efficiency in the Ugandan agricultural markets through analysis of temporal and spatial arbitrage opportunities in historical market data. The temporal and spatial arbitrage analysis aims to evaluate the amount of money that could be made following simple patterns of purchase such as buying during harvest periods, storing the produce for a given period of time and then selling during periods of planting, i.e., scarcity — for temporal arbitrage.

Our investigations were also interested in spatial arbitrage opportunities, i.e., the return on investment that would be made when buying produce from a rural market and then transporting it to a market in the urban markets. In an efficient market environment, the profit that is to be made is not expected to be persistently above the gains in the rural market environments. The return-on-investment would be expected to only cover transport and labor costs for moving produce from one market to another.

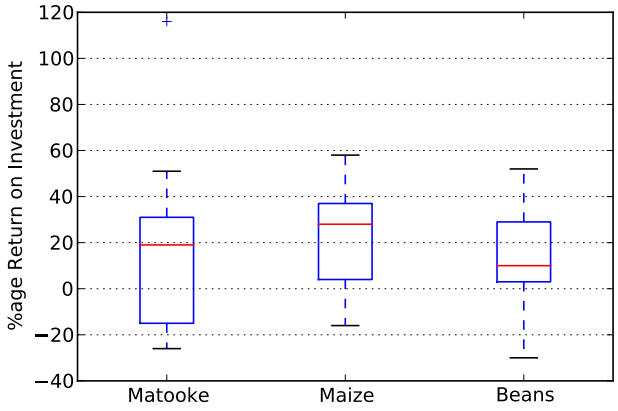


Fig. 2.4.: *Box-whisker Chart for Percentage Return on Spatial Arbitrage*

Arbitrage refers to the process of making profitable gains on investment due to differences in market prices [17]. In a developing country like Uganda, spatial arbitrage opportunities could exist as a result of differences in market prices based on locations. Prices for products in upcountry markets are mostly lower than those for products in urban markets such as capital cities. Efficient market places are expected to have price differences catering for only transportation and labor costs for moving merchandise from one market to another. Inefficient markets would however allow gains at destination markets which exceed those at source markets with all costs for movement across markets included. Market trends in Uganda tend to show relatively higher prices for commodities in Kampala than other towns in the country. This motivated an investigation into trade gains that could be achieved by moving agricultural products from upcountry markets to Kampala. On the other hand, temporal arbitrage refers to exploits in price differences at various time intervals in the market. Typically this involves hoarding products across periods which are not profitable with anticipation that sales at future dates will be profitable. In order to meet profitability, the storage and labor costs are also considered in the final selling price of the commodity.

2.4.1 Spatial Arbitrage Investigation

The market prices evaluated were obtained from Lira, Masindi, Gulu and Mbarara which are located in a radius of more than 200 kilometers from the capital Kampala. All these towns are separated from each other by distances of more than 100 kilometers. The cost for hiring a 5 tonne truck for a distance of 215 kilometers was 500,000 Ugandan shillings (UGX) in 2010; which is approximately USD 238 for the entire round trip. Approximate transportation costs for the previous years (2008 and 2009) were also used to obtain the unit transportation cost per kilometer for a kilogram of produce. The unit transportation costs were used to compute profits

	Matooke	Maize	Beans
$1^{st}Quartile$	-16.0	2.6	2.1
$Mean$	13	22.6	14
$3^{rd}Quartile$	30.1	36.2	28.5

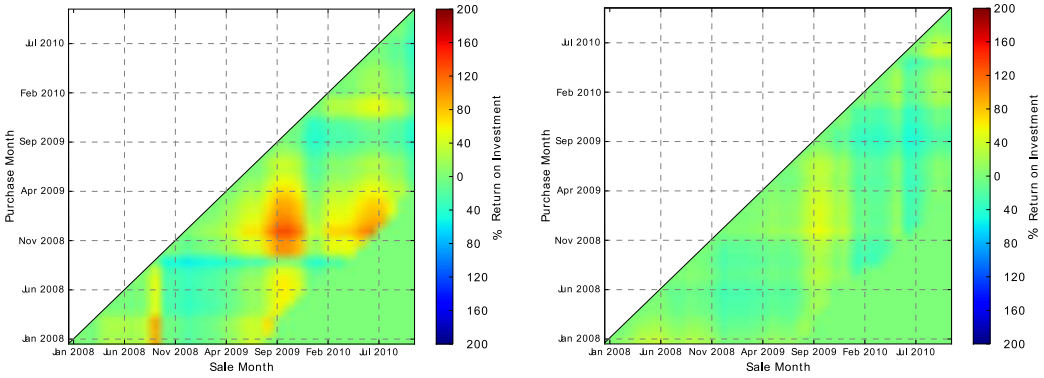
Tab. 2.1.: *% ROI comparison table*

to be made when agricultural products were to be moved from suburban to urban based markets. Our analysis evaluated the percentage return on investment (ROI) which could be achieved by transporting matooke (plantain), maize and beans from upcountry markets to Kampala.

The resultant box-whisker chart is presented in figure 2.4 showing boxplot values for return on investment for matooke, maize and beans. The choice of these products for spatial arbitrage analysis was mainly influenced by completeness of data for the period between January 2008 and October 2010. Table 2.1 presents values from the box-whisker chart indicating the quartiles and mean values for percentage return on investment when goods are moved from suburban markets to Kampala. Despite having minimum values for all the products located below the 0% mark, the first quartiles for maize and beans are above zero and the mean values for all the products are above 13% ROI. It is only matooke that has a first quartile in the negatives. The rest of the products have 2.1% and 2.6% ROI in the first quartiles for beans and maize respectively. This data shows that movement of maize from upcountry markets to Kampala is more profitable than moving matooke or beans. Of course movement of products from urban markets to upcountry markets is completely unprofitable since prices were higher in Kampala for all the three commodities (i.e., matooke, beans and maize). These trends in market prices can be linked to the fact that upcountry markets are closer to farmers than urban markets. With the third quartiles indicating gains of above 28%, spatial arbitrage values for the Ugandan agricultural produce is highly profitable. These figures indicate that the agricultural market environment lacks efficient mechanisms for communicating these opportunities hence people missing out.

2.4.2 Temporal Arbitrage Investigation

Our evaluation of historical market data for temporal-arbitrage opportunities considered products which can be stored for at least six months after harvest. The temporal-arbitrage analysis took into consideration costs for storage, labor and fumigations during the hoarding period. This chapter presents our analysis of temporal arbitrage opportunities in maize and beans in three Ugandan districts, namely; Gulu, Kampala and Masindi. Gulu and Masindi are both suburban townships while



(a) Gulu (b) Kampala

Fig. 2.5.: *Temporal arbitrage opportunities for beans in the town of Gulu and the capital city Kampala. The hue indicates the percentage profit from buying and selling beans at different times, taking into account the costs of storage. A simple trading strategy such as buying in months of production and selling in months of dry weather (For Gulu, buying in December-March and selling in June-September; for Kampala, buying in January-March and June, selling in August-October and May) can be highly profitable in Gulu, less so in the urban market of Kampala which operates more effectively.*

Kampala is an urban center. We analyzed agricultural market data from January 2008 to October 2010 for arbitrage opportunities . This data was obtained from the Famine Early Warning System Network (FEWSNET) Uganda[12].

Temporal arbitrage refers to the availability of profitable opportunities for commodities that have been stored in anticipation of obtaining higher profits at future dates. Among the agricultural products considered in this study, only beans and maize could be stored for long periods. This evaluation considers a maximum storage period of 18 months for both beans and maize. It is assumed that after 18 months the quality of beans and maize starts to degrade and to therefore become unprofitable. The cumulative storage and fumigation costs would be prohibitive for very long storage periods. The storage costs for a 5 tonne store in Kampala in 2010 was approximated at UGX 100,000. While the cost for upcountry towns such as Gulu and Masindi for a 5 tonne store in 2008 was approximated at UGX 30,000. The other important component of temporal arbitrage is “time value for money”; which we tightly couple with inflation in this context. If the products are stored for a very long periods, inflation is also likely to eat away the gains at periods which may seem profitable. Currencies in developing countries like Uganda are known for being unstable. The charts in figure 2.5 present possible dates for purchases against dates of sale for the different products. As indicated by the colorbars, the green to red color shades indicate regions of profitability while the green to blue color shades represents regions for which losses would be made given a particular combination of purchase and sale dates. The upper-left and lower-right green triangles of the charts represent regions which are logically impossible for trade. i.e. it is not possible

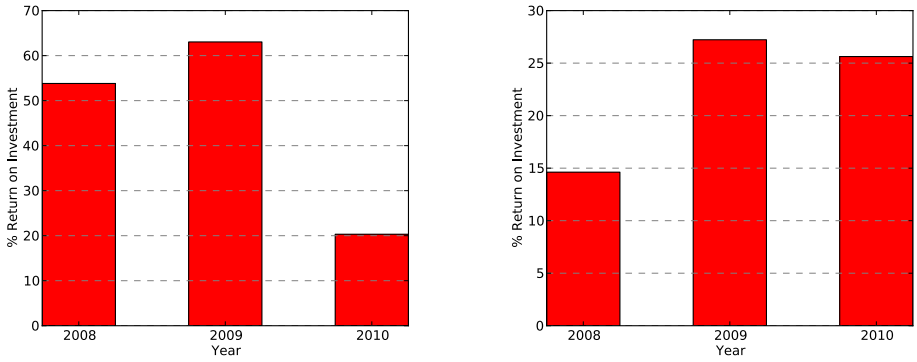
Commodity	Town	Purchase Month	Sale Month
Beans	*Gulu*	*Jan, Feb, Mar, Dec*	*Jun, Jul, Aug, Sep*
Beans	*Kampala*	*Jan, Feb, Mar, Jun*	*May, Aug, Sep, Oct*
Maize	*Masindi*	*Jan, Feb, Mar, Sep*	*May, Jun, Aug, Dec*
Maize	*Kampala*	*Jan, Feb, Mar, May*	*Aug, Oct, Nov, Dec*

Tab. 2.2.: *Temporal Arbitrage Strategies*

to sell a product before purchasing it (upper-left triangle). The lower-right green triangle indicates a region for which storage dates would go beyond 18 months.

Temporal Arbitrage Patterns

In this section we present patterns and dominant strategies for temporal arbitrage opportunities based on the heatmaps shown in figure 2.5. The price information for maize and beans was used to locate months with the lowest and highest prices in the dataset. The price information was organized in ascending order to obtain the most appropriate months for carrying out purchases and sales. The first four months (with the lowest produce prices) are considered to be purchase months and last four months are selected as sale months. The temporal arbitrage strategy for beans is to buy in the first quarter of the year and sell in the third quarter. The temporal arbitrage strategy for maize is to also buy in the first quarter of the year and to sell in the second and fourth quarter of the year. This strategy might change by a month in either direction due to seasonal changes for rains particularly in the tropical areas. As the rain seasons change, the strategies for temporal arbitrage are also affected. What remains fundamentally the same is that during harvest, the prices of agricultural produce reduce and increase during the planting season. The tropical rains in Uganda sometimes stretch into months that are predominantly known to be dry. For example, historical rain patterns, indicate June as a dry months, but this changed in 2011. Table 2.2 presents the months for which purchases and sales can be done to achieve profitable temporal arbitrage for beans and maize. The obtained strategic months for purchases and sales were used to compute possible returns on investment for the considered historical data. Figure 2.6 presents bar charts generated from profitable regions of the temporal arbitrage colormaps presented in figures 2.5. These bar charts present the best opportunities of temporal arbitrage trade from the data for maize and beans. We also notice that the dominant strategy for obtaining profitable temporal arbitrage does not work well with 2009 purchases. The high gains on purchases of 2008 are a result of maize prices almost doubling in 2009. If a trader purchased maize in 2008 and kept it for a maximum of 18 months, they would earn returns on investment of more than 50% in 2009. This strategy would not be profitable in 2009, since the 2009 prices for maize were



(a) Gulu (b) Kampala

Fig. 2.6.: *Bar charts showing return on investment for beans that are stored and sold after a period between 6 and 18 months*

almost double the prices for maize in 2010. This clearly meant that any temporal arbitrage strategy employed in 2009 would not be profitable due to prices which were significantly lower in 2010. The volatility of prices in 2009 can be attributed to high volume purchases of maize by the World Food Program (WFP) to feed displaced persons in neighboring conflict countries such as Sudan and DR. Congo http://www.newvision.co.ug/D/8/220/748036. Such high volume purchases are likely to put upward pressure on the Ugandan maize market.

Confirming our quantitative results, the findings from our interviews suggested that after goods arrive in urban markets, trading is more efficient and the potential gains from new market systems are smaller.

2.5 Analysis Summary and Conclusions

Our analysis of market inefficiency in the Ugandan agricultural market looked for spatial and temporal arbitrage opportunities for matooke, maize and beans from four markets in Ugandan townships. The spatial arbitrage investigation shows that traders can make huge profits by moving products such as matooke, maize and beans from suburban markets to the urban markets (i.e., Kampala). A trader that consistently transports agricultural produce from Mbarara, Gulu and Masindi to Kampala is guaranteed to make an average return on investment of at least 13%.

The charts presented in section 2.4.2 show that arbitrage beans and maize are highly reproducible and robust for beans and maize in Gulu, Kampala and Masindi. Evaluation of return-on-investment for beans and maize show that suburban markets (i.e., Gulu) present higher returns in temporal arbitrage than urban markets in Kampala. The trends for both spatial and temporal arbitrage show that suburban

markets are not as competitive as urban markets. The spatial arbitrage results also indicate a robust strategy for maximizing profitability by movement of agricultural products from suburban markets to urban markets.

A situation in which traders competitively exploit these arbitrage opportunities would eventually reduce the figures for returns on investment (ROI) for spatial and temporal arbitrage. The absence of competition for these market opportunities can be attributed to a lack of market information. Otherwise, profitable investment made known to traders would be shared between a large number of buyer and seller agents and eventually a market equilibrium established. Essentially, the gains on moving products from one market to another would only be enough to cover transportation costs. Likewise, returns on temporal arbitrage would only be enough to cater for storage costs. As previously indicated in a report by the Agricultural Sector Program Support (ASPS) [18], farmers or traders without market information typically get poorer deals than the well informed ones. Arbitrage opportunities available at specific periods during the year can only be exploited by well informed traders. In the absence of timely market information, it would still be difficult for most traders to learn about profitable trade opportunities.

We observe that existing techniques and tools for agricultural market support in Uganda have several shortcomings that were presented in section 2.4. The arbitrage analysis performed presents evidence for a need to develop more robust techniques and systems for agricultural trade in developing countries whose market environment is similar to that of Uganda.

3 An agent-systems approach to efficient and secure applications design

Negotiation forms a key aspect of agricultural trade (and other trade activities) in Uganda and to a similar extent other developing countries in Sub-Saharan Africa. Several researchers in agent systems have proposed various settings for agent-mediated applications. As is the case with most software systems, there are security implications for any design decisions. The automated negotiation section 3.2 of this chapter presents three example agent-mediated negotiation frameworks and investigates the implications of their design to agent-mediated applications' security. We present an overview of unique threats faced by negotiation frameworks, discuss implications of the threats and possible countermeasures.

In section 3.2 we present an introduction to agent-mediated negotiation and an overview of security aspects for negotiation frameworks. Section 3.2.1 presents design elements for agent-mediated negotiation frameworks. In section 3.2.3 we present assets and the stakeholder environment for negotiation frameworks. Section 3.2.3 presents mobility comparisons for three agent-mediated negotiation frameworks. Section 3.2.4 presents an attack model and trusted computing base for agent-mediated negotiation frameworks while section 3.3 presents possible attacker goals and attack vectors. In section 3.4 we present conclusions and discussions for security in agent-mediated negotiation frameworks.

3.1 Agent-mediated autonomic applications

To achieve a high level of automation, a robust paradigm of software configuration is needed to handle complex tasks of varying offers — in terms of price, quality and warranty among others. It is envisioned that this software paradigm would provide businesses with a platform for electronic services automation for inventory management (commodities discovery) and prices discovery. The agent systems paradigm [19, 20] provides an alternative approach electronic commerce automation.

An agent is commonly defined as "a software program that can carry out a task autonomously on behalf of its owner"[19]. In order for agent systems to facilitate e-commerce services, they are expected to exhibit generic characteristics discussed in the bulleting below. Some of these characteristics were previously presented by Wooldridge *et al.*[21].

Agents are expected to have the ability of acting independently without constantly referring back to their owner or user. In the case of e-commerce services, an agent is supposed to have the ability to make choices concerning goods or services that an owner might need depending on the owner's desires, budget and time of delivery using the initial information that was given. Researchers in Artificial Intelligence (AI) impose stronger notions to agents in which they are expected to exhibit human like characteristics such as knowledge, belief, intention, and obligation [22, 21]. Some of these characteristics are essential to agent operations, yet they can be optionally used in some environments.

- **Autonomy:** Agents are expected to have the ability of acting independently without constantly referring back to their owner or user. In the case of e-commerce services, an agent is supposed to have the ability to make choices concerning goods or services that an owner might need depending on the owner's desires, budget and time of delivery using the initial information that was given.

- **Social ability:** Agents should be able to communicate with other agents and possibly humans via some agent communication language.

- **Reactivity:** Agents should be able to respond appropriately to the prevailing circumstances in their environment and also respond in a timely manner to changes that occur.

- **Pro-activity:** Agents are expected to have the ability to act in anticipation of future goals so that their owner's objectives are met.

In this thesis we consider two types of agents; the human agents that act in an electronic market environment to achieve their consumer needs and software agents that acts in a distributed environment on behalf of their human agents to achieve specific directed goals.

The implementation of software agents follows a standard that was established by the Foundation for Intelligent Physical Agents (FIPA) (`http://www.fipa.org`). This standard enlists four major components of an agent system, namely; Message transport — for delivery of messages, Agent directory — for hosting of agents, Service Directory — for discovery of agent services published by other agents and Agent

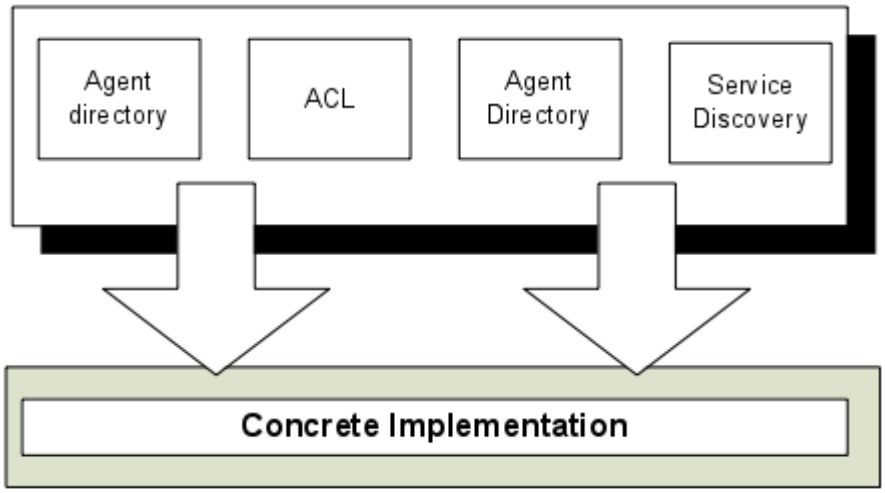


Fig. 3.1.: *FIPA-Agent Abstract Architecture*

Communication Language (ACL) — for a common language of communication between agents. This agent abstract architecture is shown in figure 3.1. FIPA provides this abstract architecture to allow for interoperability between different agent systems implementations. Concrete implementations of this architecture may differ due to optional components of the architecture.

Software agents being dynamic in nature, autonomous and proactive, are useful in ways that represent a computing paradigm natural to humans. An agent can act as a broker for its owner with minimal expenses as compared to the traditional human broker in market transactions. Information retrieval activities can be enhanced to the benefit of users if a profile concerning the searcher is known before hand. Software agents are typically expected to receive instructions from their human owners and to interact with other systems and information repositories on the Internet. It is anticipated that some of these entities could act maliciously towards each other.

This largely introduces trust questions among agents and platforms on which they execute. To explain the trust problem in the agent paradigm further, we consider an example of a person who wishes to purchase items from one of the shops in her new neighborhood. This kind of buyer would wish to choose a reliable shop among those available that meets her financial (pricing, discounts and promotions) and other set constraints such as branding, shopping environment and customer care. It would be wise for such a consumer to consult with people who have stayed in that place long enough in order to obtain information concerning the shops or markets. Such a customer is expected to have a fair level of trust of her neighbors to accept the information and recommendations being suggested. In such a situation, the consumer is faced with a trust challenge. Such a situation is similar to what agents

face whenever they seek reputation information from new sources that could be unreliable or would have been compromised by malicious elements.

Due to the increasingly sophisticated nature of attackers, reputation information is sometimes altered to benefit individual agents and at times wrong information about agents is sent to reputation repositories. Attackers that carry out such actions are technically referred to as strategic liars. Additionally, most trust models have been generic in nature, and thus giving rise to confusing trust contexts. Confusing trust contexts arise in cases where one entity assumes certain parameters for trust, yet those parameters are insignificant or irrelevant for the prevailing environment. Examples of strategic liars and confusing trust contexts have previously been presented in literature[23, 24]. Such challenges require improvement in trust management models to close existing gaps in agent-mediated e-commerce environments. Additionally, existing security techniques need to be improved to cater for the unique processes of agent-mediated e-commerce.

3.1.1 Agents in b2c e-commerce

B2C e-commerce which involves selling of goods and services to a consumer by a business enterprise is very popular nowadays, since many people have recognized the convenience of shopping at the click of the mouse. However, as more people move towards on-line shopping or B2C e-commerce, so is the need to improve software technologies to meet the new demands of customization, efficient retrieval of information and timely deliveries of goods and services.
A Consumer Buying Behavior (CBB) model in which agents act as mediators in the five stages of *need identification*, *product brokering*, *buyer coalition formation*, *merchant brokering and negotiation* is shown in Figure 3.2. To illustrate functional behavior of the CBB model, let us consider an example of an individual who wishes to buy a text book concerning Ugandan history using an agent-mediated system. The consumer is expected to instruct his software agent to search for a book on Ugandan history that was published less than 4 years ago, costing no more than $50 and should be new with hard cover. Armed with this information, the agent moves to available on-line markets dealing in book sales and searches for availability of books costing no more than $50 in addition to all the other attributes that the agent owner needs. Initial results may indicate availability of books selling at a price higher than $50, so the agent sets out to look for more markets that could probably be cheaper — all these initiatives are expected to take place without the agent-owner intervention.

The software-agent could additionally monitor current shops for short-term price reductions in addition to negotiating for better prices. The software-agent could also monitor auction markets for probable cheaper options — without actually

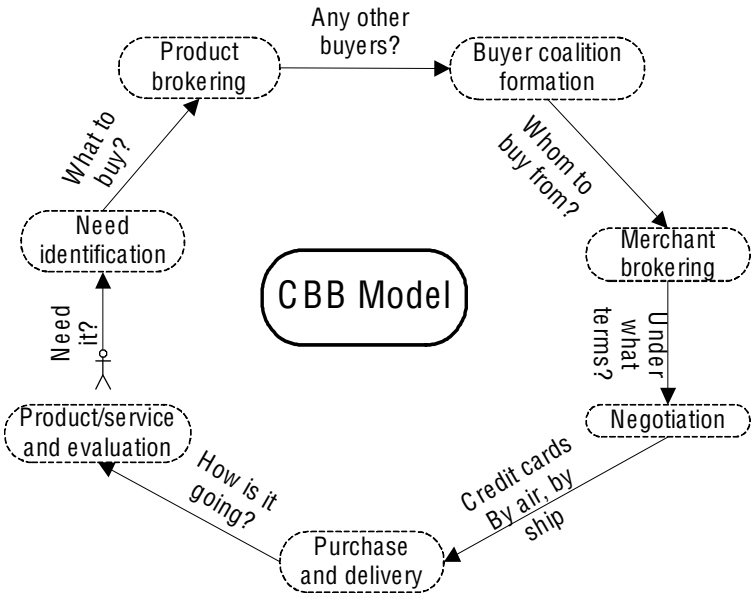


Fig. 3.2.: *Consumer Buying Behavior Model (Adopted from [25, 26])*

performing a bid since such an action would require committing its master's money. The software-agent could also have an option of relaxing requirements of its master; these options may include considering books on Ugandan history that are more than 4 years old, books that are not hard-covered or even secondhand books that could be cheaper. The agent could also try to find out other agents with whom a coalition can be formed to buy a bigger package of books at a reduced price. The agent can then report back after performing negotiations on the availability of books concerning Ugandan history ranking them in the order of preference based on the master's preferences. The owner has possibilities of making a choice out of what the software agent has provided, or even rejecting them and instructing the agent with new requirements or constraints.

3.1.2 Advantages of using agent-mediated systems in e-commerce

Since software-agents have the ability to act autonomous, socially, reactively and pro-actively, their use in electronic commerce presents several advantages and improvements in open distributed environments. In the listing below, some of the advantages that are attributed to agents in electronic commerce are presented.

i. Automation: Ability for agents to act autonomously presents many opportunities for enabling automation in agent-mediated e-commerce.

ii. Responsiveness: Since agent systems have *reactive* and *pro-activeness* properties, they are expected to facilitate timely responses to changes in their environment and business markets.

iii. Flexibility: Research[22] from the AI field agrees with the fact that multi-agent systems can actually be conceptualized and developed with human like notions of knowledge, belief, intention and obligation which certainly implies that they (agents) can act flexibly in the environments in which they participate.

iv. Scalability: As more information grows on the Internet currently available paradigms will most likely fall short of the new demands. Since software-agents can process information from the source and reason about its relevance to the agent owner and negotiating for goods and services without communicating very often with the sender, this paradigm scales well to the growing information in open distributed environments.

v. Economical: Resource utilization is low (in terms of bandwidth) for agent-mediated electronic commerce since agents minimize the amount of communication and message exchanges along communication channels.

Technologies for supporting development of agent system are already in place. Several languages are available for supporting interactions between agents such as eXtensible Markup Language (XML)[27] and Agent Communication Languages (ACL)[28] that are used to code information and services in meaningful structures that agents can easily understand and process.

3.1.3 Security challenges in agent-mediated consumer buying behavior models

The deployment of agent systems in large-scale open distributed environment systems presents a host of digital security challenges. In the enumeration below, we present some of the challenges that are likely to be faced by agent systems in electronic-commerce systems.

i. **Availability** - Agents in E-Commerce systems represent stake holders that have several objectives some of which could be malicious or depriving to other participants.

ii. **Non-repudiation and Identity Management** - Agents operating in open distributed environments have the ability to perform various tasks and later on obtaining a different identity to hide their previous actions. In an e-commerce environment, agents could accept payments for goods that they may not deliver

after receiving payments. Additionally, selling agents can even deny having ever received payment for goods to be delivered to customers.

iii. **Integrity** - Information that is carried by agents in the electronic environment needs to be protected from malicious elements that may want to destroy it or even alter its meaning.

Furthermore, due to the increasingly sophisticated nature of attackers, reputation information is sometimes altered to benefit individual agents and at times wrong information about agents is submitted to reputation repositories.

iv. **Privacy and Confidentiality** - As agents traverse networks to fulfill their objectives, they carry information with them that usually represents needs of their owners. This information is used as a basis for interaction and service negotiation with other agent systems in the network. In many cases (and for several different reasons) agent owners would wish to keep all or part of this information private.

v. **Strategic Liars** - Agents in the CBB model cannot be expected to always behave truthfully. Agents could for example lie about their preferences when interacting in the market, they could vote untruthfully when indicating their liking or dislike for commodities in the market.

Security requirements such as confidentiality, integrity and availability are inherently required for all electronic-commerce paradigm even with out the application of agent systems.

3.2 An agent-mediated negotiation framework

In recent years, agent systems have been used in various real world applications such as distributed planning, scheduling, e-commerce and resource management. A key component to most agent-mediated applications in e-commerce, is the negotiation process through which entities participating in a transaction find a position of agreement in the event of a discrepancy. Negotiation has previously been defined as dynamic processes in which parities involved exchange offers, make concessions, or influence each other in order to reach an agreement[29]. With the advancement of agent systems technologies, much research work has been done in integrating automated negotiation [30, 31] in agent-mediated applications. The minimum requirement for automated negotiation in agent systems is the ability to construct proposals and respond to requests.

Negotiation frameworks provide building blocks for facilitating automated negotiation processes. Functional requirements for negotiation frameworks have previously been defined by Mobach et al. [32], and the design of a negotiation framework for AgentScape platform [33] was based on these requirements. However, as is the case with several other complex software systems, several researchers have mainly focused on functional requirements and either ignored security completely or only considered it after advanced stages of functional designs. This situation is true for the negotiation framework suggested by [32] and MAGNET by Collins et al.[34, 35]. Some of these frameworks have considered implicit and explicit assumptions such as participants in the protocol being rational and not behaving maliciously towards one another. In a practical open distributed environment, such assumptions would be very strong due to high possibilities of a negotiation framework being compromised by internal and external attackers.

In the context of negotiation frameworks, we introduce a distinction between internal, external and agent attackers.

- *Internal-attackers* refers to individuals and or entities that could be participating in the negotiation protocol. Such attackers could be people or software agents that are performing a bilateral trade or bidding in an auction.

- *External attackers* on the other hand refers to entities that are not participating in the negotiation protocol but have the ability to affect normal operations of the negotiation framework.

  Such attackers are assumed in the Dolev-Yao [36] attacker model to have the ability of listening on the communication channel, intercept and analyze messages being exchanged between communicating parties.

- *Agent-attackers* have stronger abilities than the internal and external attackers to perform malicious activities on the negotiation framework. A malicious platform which has the ability to terminate an agent or destroy its data is an example of agent attacker.

In the design of negotiation frameworks, various application settings have been proposed but no comparative discussion on the effect of these application organizations to the security of the negotiation frameworks has been done. We consider three negotiation frameworks for this comparative study.

3.2.1 Structure of an agent-mediated negotiation framework

As previously indicated in the introduction section, negotiation frameworks facilitate automated negotiation processes. In this section we present details of negotiation building blocks, the activities involved, stakeholders and their software architectures. Automated negotiation frameworks are mainly built around three structures [30], namely:

- *Negotiation Protocol*: The protocol defines a set of rules and procedures that have to be adhered to by parties participating in a negotiation. In e-commerce, negotiation protocols ensure that participants adhere to the trading rules. In the example of auction markets, a negotiation protocol will impose rules on participants for the type of auction (Dutch, English or Vickrey) being carried out.

- *Negotiation Objects*: These are the range of attributes over which participants in negotiation can make choices. Such issues may include price, quality, model of item and service agreements.

- *Agent Decision Making Model*: The agent decision making model works within the provisions of the negotiation protocol and negotiation objects available. The quality of the agent's decision making model determines the level of success that the agent will achieve.

3.2.2 Examples of agent-mediated negotiation frameworks

We hereby present three example agent-mediated negotiation frameworks to illustrate differences in agent-mediated architectures. These negotiation frameworks were chosen because of their differences in architectural design. In order to have easy references in the chapter, new labels (names)[1] are assigned to the two negotiation frameworks without short names.

TrinAge

This negotiation framework relies on three agents (Controller Agent (CA), Worker Agent (WA) and Itinerary Register Agent (IRA)) [37, 38] to carry out the negotiation process on behalf of the consumer; The negotiation process involves a client (represented by three agents) interacting with shortlisted suppliers on certain parameters (negotiation objects) until they reach an agreement or abort the negotiation. The

[1] The framework developed by Mobach et al. [32] is referred to as **MoVir**, **TrinAge** refers to the framework developed by Al-Jaljouli et al. [37, 38] and **MAGNET** is maintained for MAGNET [35].

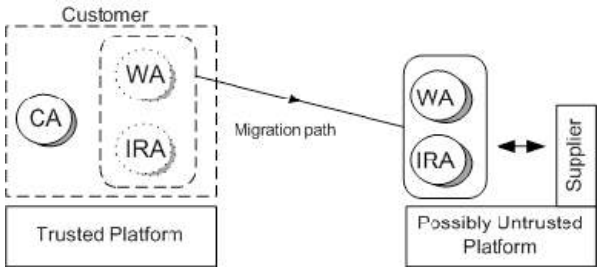


Fig. 3.3.: *TrinAge Architecture*

framework depends on a trusted host to provide a trusted computing base for performing business critical services such as setting negotiation parameters, evaluation of offers and decision making [37].

- The Controller Agent (CA) stores critical data such as the list of offers, expiry time of the bid, scoring and decision functions.
- The Worker Agent (WA) stores non-critical data and tactic functions which form the agent's decision making model.
- The Itinerary Register Agent (IRA) stores addresses of the visited suppliers and the time (t) at which the agent got executed at the service provider's host.

TrinAge assumes a scenario in which agents (WA & IRA) representing a customer move through public networks and to possibly untrusted service provider hosts in search of offers. The framework aims to achieve confidentiality of negotiation strategies and decision making model by separating the handling of critical and non-critical data into two agents (CA and WA respectively). Figure 3.3 below, presents an overview of the TrinAge architecture. We note here that the supplier (service provider) entity is not an agent.

MoVir

Mobach et al. [32], designed a negotiation framework in which consumers negotiate with service providers through mediators. In this framework, consumers are presented with services aggregated in virtual organizations. The creation and management of virtual organizations is performed outside the negotiation framework. Consumers can negotiate with several mediators and mediators simultaneous negotiate with several service providers. Service provider details are hidden from the customers by the mediators that provide an aggregated point of contact. The application framework is very dynamic, involving service providers leaving and joining virtual organizations at any time. The framework consists of a Consumer

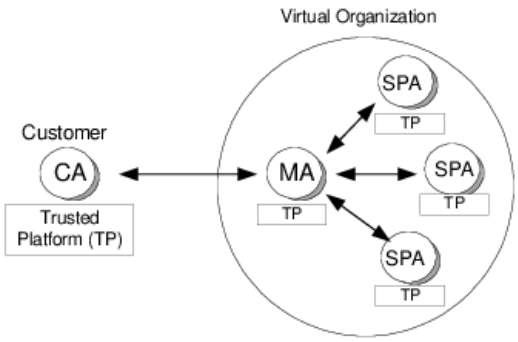


Fig. 3.4.: *MoVir Negotiation Framework*

Agent (CA), the Service Provider Agent (SPA) and Mediator Agent (MA) whose roles are briefly explained below:

- The Consumer Agent (CA) represents the human buyer in the negotiation process. Consumer agents initiate the negotiation process by looking for services. Consumer Agents locate mediators and the services they offer through some external services such as directory services [39]. The CA performs multi-attribute negotiations with one or more Mediator Agents (MA). Customer Agents may have to migrate to Mediator Agent platforms in order to accomplish their tasks.

- The Service Provider Agent (SPA) is responsible for providing goods and services that are sought after by consumer agents. Depending on the service type, the SPA may be required to migrate to the Mediator Agent (MA) platform to provide the requested service.

- The Mediator Agent (MA) represents a virtual organization of service provider agents that are governed by specified policies. Each virtual organization is administered by service policies that are different from other virtual organizations.

MoVir assumes an environment in which the customer agent and agents in the virtual organization (mediator and service provider agents) execute from trusted platforms. Figure 3.4 below presents an overview of the MoVir negotiation framework.

MAGNET

The Multi-Agent Negotiation Testbed (MAGNET) is an architecture that was developed to provide support for agent interactions in trade negotiations. MAGNET supports automated contracting, negotiation and monitors execution of contracts in business transactions [40, 35]. MAGNET provides an automated marketplace

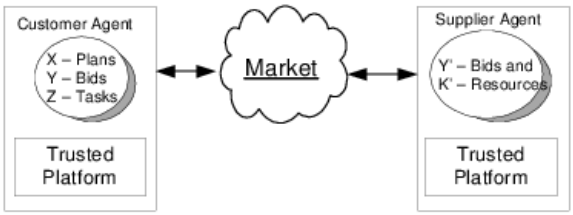


Fig. 3.5.: *MAGNET Architecture*

through which software agents represent their owners in an auction. In order for the consumer agent to fulfill a set of tasks, it generates a plan from the tasks and solicits for help from supplier agents in the market. Essentially, this framework comprises of two agent roles; the customer and supplier roles.

Figure 3.5 below presents an overview of the MAGNET architecture in which a trusted third party (market) mediates all communication between customers and suppliers participating in an auction. The customer agent sends out Requests For Quotes (RFQ) to suppliers in the market and a set of suppliers with the requested services would reply with an indication of prices and any-other constraints such as time. After the customer agent has received the bids, it evaluates them based on predefined parameters such as price and time and then selects the most optimal bids. After the bids have been selected, successful suppliers are notified and the Execution Manager is called to oversee completion of the negotiation process with the shortlisted suppliers. The Planner is called to renegotiate offers which are then sent to the Bid Manager for re-assignment to the Execution Manager. The execution manager, planner and bid manager are components of the customer agent.

3.2.3 Composing the underlying framework

In table 3.1 below, we present a summary table comparing assets that can be found in the three negotiation frameworks. The items presented are a representation of underlying structural details in the negotiation frameworks.

Mobility Comparisons

Mobility features are critical to security of agent systems. This is because agents may migrate to malicious platforms. Agents executing on maliciously platforms face greater risks of having security properties of their code or data being compromised. Due to design differences in negotiation frameworks, some agents are expected to migrate to other platforms in order to accomplish their tasks while in some frameworks migration is not expected. Moreover, in the case of TrinAge, the service provider is non-agent. Table 3.2 below presents comparisons of entities in the

TrinAge	MoVir	MAGNET
Controller Agent List of offers, shortlist of vendors, negotiation parameters Worker Agent Request for offers, User preferences, user predefined constraints Itinerary Register agents Shortlist of vendors, time of execution at remote host Vendor List of offers, Expiry time of offers, offer parameters (such as price and discount constraints)	Customer Agent Requests for offer, shortlist of offers Mediator Agent List of offers, list of service providers, negotiation requests sent to service providers, contracts with service providers Service Provider Agent Service adverts, contracts with mediators	Customer Agent List of tasks, user preferences (price, time constraints) Request For Quotations (RFQ), Supplier Agent RFQs, Offers Market (moderator) RFQs, Bid messages

Tab. 3.1.: *Comparison of assets in the negotiation frameworks*

Framework	Entities Involved		Agent?	Mobile?
TrinAge	Customer	*Controller*	Yes	No
		Itinerary Register	Yes	Yes
		Worker	Yes	Yes
	Supplier		No	No
MoVir	Customer		Yes	Yes
	Mediator		Yes	No
	Service Provider		Yes	Yes
MAGNET	Customer		Yes	No
	Market		No	No
	Supplier		Yes	No

Tab. 3.2.: *Comparison of entities and mobility in negotiation frameworks*

various negotiation frameworks which are agents, non-agent, mobile and non-mobile components.

Stakeholders and assets in negotiation frameworks

The presented configuration of agent-mediated negotiation frameworks reveals that they (TrinAge, MoVir, and MAGNET) are comprised of a customer and service provider at a minimum. In some circumstances, such as MoVir and MAGNET, a moderator or trusted third party is used to oversee and facilitate activities between customers and suppliers. In addition to the customers, suppliers and moderators, agent-mediated negotiation frameworks consist of other assets such as negotiation protocols, negotiation objects or parameters and decision making functions that

need to be protected. Attacks on these framework elements could substantially alter behavior of the negotiation framework.

Automated negotiation frameworks would typically have customer agents carrying negotiation parameters and decision making functions which are used during execution of the negotiation protocol. Customer agents are responsible for receiving bids from suppliers. Adversaries in the environment will attempt to compromise these assets either for their own profit or to fail goals of legitimate participants. The following common target assets have been identified in the three negotiation frameworks:

a. Agents that are participating in the negotiation.

b. Offers or sometimes referred to as Asks.

c. Bids submitted in response to a request for offer or quotation.

d. Negotiation objects or parameters.

e. User and market predefined constraints such as delivery time, bid closing time and expiry time of offer.

f. Shortlist of suppliers to be considered by the customer.

g. Contracts between suppliers, market/moderators and customers.

3.2.4 Attack model and trusted computing-base in automated negotiation frameworks

In order to bring the attack model for an agent-mediated framework into context, we model interactions between collaborating agents using figure 3.6. Figure 3.6 provides a high level representation of possible interactions between agents in negotiation frameworks. It illustrates a scenario in which Agents A and B might be involved in a bilateral negotiation with a supplier agent. Agents A and B are legitimate participants in the transaction with a supplier, but agent B may wish to cheat agent A using the knowledge he or she possess about the negotiation protocol. In the listing below, we describe the three forms of attacks identified in negotiation frameworks.

i. **Malicious Agents**: This type of attacker has privileges of legitimate participation in the negotiation. The attacker has the ability to study the negotiation protocol and maliciously use this information against other participants in

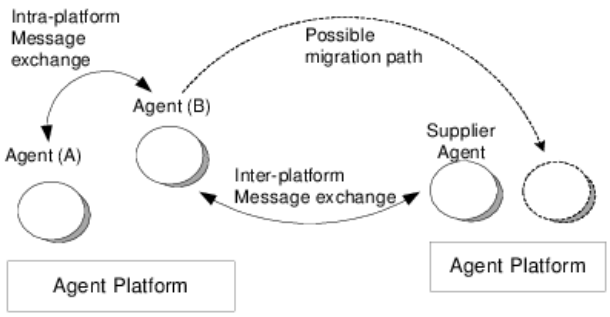


Fig. 3.6.: *Overview of attack model for agent-mediated negotiation frameworks*

the negotiation. A customer agents may collude in the market to unfairly out compete other agents.

ii. **Malicious Platforms**: This is a powerful adversary that can compromise confidentiality, integrity and availability of the agent and its data. These attackers can have the ability to intercept intra-platform messages, to destroy the agent and its data structures.

iii. **Dolev-Yao Attacker**: In the Dolev-Yao threat model [36], an attacker is assumed to have the ability to listen on the communication channel and can intercept messages being exchanged between two parties. In our scenario of negotiation frameworks, such attackers can intercept intra-platform and inter-platform message exchanges.

These three agent frameworks presented in subsection3.2.2 are used to highlight differences in threats that may occur in agent-mediated negotiation frameworks when certain design decisions are made.

Unlike TrinAge, MoVir and MAGNET assume a trusted platform for execution of all participating agents. TrinAge assumes a scenario in which customer agents may visit untrusted platforms and thus provides protection mechanism for survivability of the customer agent by splitting functionality between three agents. A malicious platform could however still destroy an agent that migrates to a hostile platform.

Table 3.3 presents a summary of attacks that are possible with the three negotiation frameworks based on their design (see section 3.2.1) and stakeholders (see section 3.2.3) involved. MoVir and MAGNET assume a trusted platform for agent execution, hence eliminating possibilities of an agent attacker. TrinAge caters for situations in which the platforms are not trusted. The Worker and Itinerary Register Agents are tasked with the risk of collecting information from untrusted service provider platforms and returning to a trusted platform to perform business critical functions.

Framework	Entities Involved	Malicious Agent Attacks?	External Attacker (Dolev-Yao)?	Malicious Platform Attacks?
TrinAge	*Controller Agent*	Yes	No	No
	Itinerary Register	Yes	Yes	Yes
	Worker Agent	Yes	No	Yes
	Supplier	Yes	No	No
MoVir	Customer Agent	Yes	Yes	No
	Mediator Agent	Yes	Yes	No
	Service Provider Agent	Yes	Yes	No
MAGNET	Customer Agent	Yes	Yes	No
	Market Moderator	Yes	Yes	No
	Supplier Agent	Yes	Yes	No

Tab. 3.3.: *Comparison of attack models against negotiation frameworks*

3.3 Kinds of attacks and countermeasures

This section presents various threats that can be faced by the negotiation frameworks and the means by which adversaries would achieve their goals. Confidentiality, Integrity, Availability and Non-repudiation (CIAN) are well studied security properties for digital systems; this section presents an overview of attacks that could be used to compromise these security properties in reference to the assets and stakeholders involved. However, because of threats which required more details than can be achieved with CIAN, additional requirements are presented in the subsections which follow.

3.3.1 Confidentiality attacks

In all the negotiation frameworks considered, message exchanges are involved and participants would desire to keep their contents confidential either for privacy reasons or to enable them compete fairly with other participants. Such messages include requests for offers, requests for quotations, negotiation parameters, user predefined constraints, bid messages and contracts with suppliers and market moderators. Additionally, an attacker might be interested in maliciously disclosing identities of agents that participated in a particular transaction. Adversaries could also be interested in knowing about details of the bids before the auction closing time so that they make better bids than their competitors.

Confidentiality countermeasures

Faced with threats of malicious disclosure of agent identities, anonymity can be used to prevent this threat from happening by hiding identities of participants. However, almost all transactions involved in agent-mediated negotiation would require some form of accountability and/or authentication. It would be inappropriate to have true anonymity yet agents may have to be accountable for some of their actions.

We instead recommend pseudonymity for such environments. Which provides pseudo names to agents so that they actions cannot be authenticated and recorded. Pseudonymity is also relevant for frameworks that reply on agent reputations to build trust models. Reputations cannot be built in environments that do not have any reference point to past activities of agent identities. An example of security schemes using pseudonymity (referred to as virtual identities) have previously been suggest by [41] and [42]. Practical implementations of pseudonymity have been achieved in AgentScape [43] platform by use of agent handles as pseudonyms to support authentication and anonymity in payment schemes.

Other issues of confidentiality also arise for example in auctions whereby information about the bids is not supposed to be revealed to participants until the end of the auction. Techniques such as time-lock puzzles and timed-release cryptography [40, 44] have been suggested in systems like MAGNET to prevent such threats. Lastly, encryption of messages, use of signed digital certificates for communication between negotiating parties and mutual authentication would also prevent eavesdropping, spoofing and man-in-the-middle attacks in negotiation frameworks. These techniques can be implemented using the Transport Layer Security (TLS) protocol [45]. However, challenges still exist in regard with threats from internal attackers that may also have valid certificates with the Certificate Authority and can establish legitimate connections between targeted communicating parties.

3.3.2 Attacks against integrity

Integrity threats are targeted at changing contents of messages, agent code and other objects such as negotiation parameters, closing time of bids and offers in order to suite interests of an adversary. An attacker could for example change contents of the list of shortlisted suppliers in order to prevent the customer from considering certain suppliers in the final negotiation phases. In case the bid closing time or expiry time of an offer is changed by an adversary, participants would not be able to rightly accomplish their goals. A more complicate integrity problem also exists in frameworks which support mobility. An adversary could for example launch a man-in-the-middle attack which could be used to alter the agent's code. If the code

checksums are not protected, the attacker could even recompute the checksums and insert a new version of a compromised agent.

Integrity countermeasures

As indicated is subsection 3.3.2 agent-mediated negotiation frameworks face integrity threats against their own code and the information they carry. Countermeasures to integrity threats can be classified into detection and prevention categories. Majority of the techniques discussed here are detection techniques for tampering either on agent data or code. TLS protocol implementations can be used to guarantee integrity of messages and mobile agent code against an external attacker but will not protect the negotiation framework against an internal attacker. Similar to attacks on messages, man-in-the-middle attacks can be launched by an internal attacker on mobile-agent code. Mobile agent code could be changed and new versions of agent code inserted by adversaries during transactions. Such threats can be detected by signing agent code and data objects. Ideally agent code should be signed by the agent creator/developer and the data objects digitally signed by the agent owner. Security mechanisms involving signing of code and objects would require a Public-Key Infrastructure (PKI) for retrieve decryption keys. A PKI is also important for mutual authentication and providing secure communication channels using TLS between communicating parties.

A distributed trust technique was proposed by [46] to maintain integrity of migration paths so that in case of deletion or tampering with agents' data or code, the malicious platforms can be held accountable. The other two known mechanisms for recording and protecting migration paths involve (a) using a centralized trusted third party to authorize and keep track of migration paths and (b) using signature chaining without a trusted third parties [47]. The distributed trust technique provides better mechanisms for protecting migration path information. It avoids the overheads of a trusted third party and mitigates problems involved with storage of signatures of migration paths inside the agents themselves by using signed waivers of migrations path information from previously visited hosts.

All negotiation frameworks reviewed in section 3.2.1 implicitly assume trust for the agent. However, this assumption cannot always hold since agents may come from malicious customers or they (agents) might have been compromised before arrival at the execution platforms. Sand-boxing or jailing [48] provides one of the well tested techniques for protection of platforms against execution of untrusted code. Model Carrying Code (MCC) [49] is another approach which provides a practical approach to monitoring of untrusted mobile code execution on agent platforms. Compared with Proof Carrying Code (PCC) [50], MCC overcomes limitations of verifying binary code after application deployment [49]. The mobile-agent is expected to present a

high-level model of its security-related behavior to the agent platform to be verified for conformance with the security policies of the platform.

3.3.3 Attacks on availability

Denial of service attacks are a threat to proper functionality of all services involved in the agent-mediated negotiation framework. Survivability of an agent is at a higher risk when the negotiation framework supports mobility. Unlike TrinAge, MoVir and MAGNET assume a trusted platform for execution of all participating agents. TrinAge assumes a scenario in which customer agents may visit untrusted platforms and thus provides protection mechanism for survivability of the customer agent by splitting functionality between three agents. As previously indicated in Table 3.3, an Agent attacker could still destroy an agent that migrates to untrusted platforms. Moreover, other assets such as offers shortlisted from suppliers could be removed from the shortlist by a competing supplier. Messages exchanged during the negotiation process could be hijacked by an adversary so that they do not reach intended participants.

Publication of services in the publish/subscribe system such as the one used in MAGNET and MoVir could be done in a such a way that some participants do not get the information timely. Such a scenario could lead to unfavorable competition among participants in-case time constraints are involved in a bid. Some adversaries could also publish bogus bids into the publish/subscribe system or even replay bids from other suppliers to damage their reputation or that of the entire market. In circumstances where negotiation frameworks rely on directory services to discover markets or suppliers (e.g. MoVir), a compromise to a directory service would imply that the suppliers will not be discovered. This kind of attack is possible with MoVir where a mediator agent aggregates services from suppliers in a virtual organization and assumes that all parties in the negotiation framework are trusted. Attackers could also use more resources than they are authorized on service provider platforms. Such actions would lead to denial of services to other agents accessing related services.

Availability countermeasures

As a first step for protecting agent-mediated systems against availability threats, detection mechanisms based on the techniques discussed in subsections 3.3.1 and 3.3.2 should be put in place. Security mechanisms such as recording of migration paths using distributed trust can be used for accountability in case agent gets changed or destroyed.

It is also critical to manage privileges of agents on agent platforms to prevent denial of service attacks. Schemes such as Role Base Access Control (RBAC) [51] have been implemented in agent platforms such as AgentScape to manage roles and access to system resources. However, this mechanism also introduces challenges to provision of anonymity services to agent-mediated negotiation.

Threats of agents being destroyed when they migrate to malicious platforms have not been adequately dealt with. Most security mechanisms provide for detection of agent failure and tampering, but no solid solution has been presented for graceful failure or protection of data owned by the destroyed agent. A faulty tolerance technique based on replication of an agent had previous been presented by [52]. However, complete agent replication schemes impose computational overheads on agent platforms.

The last problem we consider in this category of threats is annoyance attacks in which an attacker may make bogus submissions to the publish/subscribe system. Agent platforms such as AgentScape [51], JADE [53], SeMoA [54] and Cougaar [55] have all implemented identity management schemes to facilitate authentication and authorization requirements. However, only AgentScape has implemented partial anonymity services which can be used for authentication and authorization. We refer to the anonymity services provided by AgentScape as partial because they use agent handles (which is a hash of the global agent identifier) which can be traced back to the true identity of the agent by an authorized administrator. MoVir framework was implemented using AgentScape [56, 57] platform and thus utilizes all security services in AgentScape. The question of whether an agent should be allowed to submit offers or not to a publish/subscribe system or to a mediator agent as is the case with MoVir is largely a trust issue. The agent systems research community [58] has largely considered reputation models for answers to trust relations.

3.3.4 Non-repudiation attacks

Non-repudiation means that there is proof for actions that were performed by participants in a negotiation. A customer should not be able to deny having submitted a request for an offer from suppliers. The negotiation framework should also ensure that the supplier cannot repudiate the responses they made to their customers. In MoVir, a mediator agent could deny having received service subscriptions from some suppliers. In order to achieve non-repudiation, some form of identification is required, the negotiation framework should additionally provide protection for identification information so that adversaries do not use it to violate confidentiality requirements.

Repudiation countermeasures

Psuedonymity can be used to maintain partial anonymity and accountability for agent actions when participating in negotiations. Use of reputation models in such environments works as good incentive to correct behavior to participating agents. Digital signatures can be used to provide proof that a certain party sent a message. A message sender cannot claim that they did not send a message that they signed unless their private key was stolen. Identity Management Systems for agents in the execution environment have been implemented for example in AgentScape to prevent an agent owner from repudiating ownership of an agent. Agents are identified by the middleware using a global unique identifier (GUID). The GUID is private to the middleware and cannot be used by elements in the agent environment to send or receive messages from the agent. Instead a hash of the GUID concatenated with a counter is generated and published to a directory service for public access. All agents in AgentScape are signed by the agent owner to provide non-repudiable ownership. Unlike MoVir whose security mechanisms are based on AgentScape middleware, TrinAge and MAGNET frameworks do not have security mechanisms for providing both anonymity and accountability services.

3.3.5 Collusion attacks

Formation of coalitions in negotiations can be advantageous to both suppliers and customers. Customers get a chance to bargain for lower prices due to expressions of higher demand (with bulk purchases) for products and services. On the other hand suppliers get an opportunity for bulk sales. However, unsupervised coalitions can also be used by colluding buyers to unfairly out-compete other participants. In situations of bidding, suppliers may not receive competitive prices if customers collude to purchase services at low prices. All the three negotiation frameworks studied are vulnerable to collusion attacks.

Collusion countermeasures

A solution to collusion attacks based on public verifiability of winner determination data in case of a dispute was presented by Shi et al. [59]. Participants with secret keys to winner determination data would be able to retrieve the decision making data. This solution is inadequate and cannot address the problems presented in subsection 3.3.5 since collusion trails cannot be found in decision making data.

Requirements	Security Mechanisms
Confidentiality (Identities and Requests/Bids)	Encryption, Pseudorymity, Timed-release cryptography
Integrity (Messages and Agent Code)	Digital signatures and certificates, migration paths
Availability and Fairness (Agent and Messages	Role-based access control (principle of least privilege), Sandboxing techniques, migration paths, Reputation models
Trusted Service Discovery	Authentication and authorization techniques, Reputation models
Non-repudiation	Authentication, digital signatures and certificates
Collusion Prevention	Reputation models, "Public" verification of information

Tab. 3.4.: *Security Requirements and Mechanisms*

3.4 Discussions and conclusions

This section has taken a detailed study of assets and stakeholders involved in the negotiation frameworks and investigated possible risks that would be experienced in the event of an attack. An attack model that is based on internal, Dolev-Yao and Agent attacks is discussed and applied to the three negotiation frameworks. Standard cryptographic techniques are available to prevent most Dolev-Yao based attacks, but the design choices for implemented security protocols may introduce vulnerabilities. This scenario can be found in the security protocol presented by Jaiswal et al. [40] to mitigate weakness in MAGNET, but did not cater for replay attacks as noted by Shi et al. [59]. TrinAge makes effort to protect components of the customer agent against malicious platforms, but does not completely achieve this because the information collected by the worker and itinerary register agents (which visit hostile platforms) could still be destroyed with these two agents. TrinAge further provides mechanisms for detecting when an offer has been removed from the collection of offers, but does not provide prevention mechanisms against this attack before offers are submitted to the controller agent. The publish/subscribe system proposed in MAGNET provided a more secure centralized control for market transactions than the mediator agent in MoVir and the mobility functionality in TrinAge. In table 3.4, we present a summary table mapping security requirements in negotiation framework to various security mechanisms. As much as this chapter presents security mechanisms that can be used/deployed to mitigate threats, it does not address weaknesses in these security mechanisms. Security problems that exist with reputation models, publish subscribe systems, distributed trust and security protocols are addressed in the second section of this chapter.

4 A privacy preserving approach in electronic-trading applications

In section 4.1 we present an introduction to publish-subscribe systems, their relationship to the consumer buying behavior model and security requirements for their deployment in a multi-agent environment. Section 4.3 presents related work for secure publish-subscribe mediated environments and their shortcomings. In section 4.4 we present a secure design for a publish-subscribe mediated environment and a description of security protocols and cryptographic hash functions needed to achieve this goal. We perform an evaluation of the proposed security protocols and security mechanisms in section 4.7. We present conclusions to this study in section 4.8.

4.1 Privacy and confidentiality in consumer buying behavior models

Publish-Subscribe systems are commonly used in highly dynamic environments and systems to support many-to-many (asynchronous) service and communication requirements. Such electronic markets typically involve suppliers advertising their goods and services in a common electronic repository. Customers in the environment would then search for these goods and contact suppliers for completion of the transaction. A prominent model for supporting customers and suppliers in autonomic markets was previously been defined by Guttman et al. [60, 61] in a *Consumer Buying Behavior (CBB) model* mediated by agents. Figure 4.1 presents the seven stages that constitute a CBB model. The seven stages of the CBB model are: (1) *need identification*, (2) *product brokering*, (3) *buyer coalition formation*, (4) *merchant brokering*, (5) *negotiation*, (6) *purchase and delivery* and (7) *product or service evaluation*. We note here that not all stages described in the CBB model are mandatory for consumer transactions. Some transactions may-not for example involve negotiations or formation of coalitions. In this chapter, we consider privacy, confidentiality and integrity challenges for an electronic market in which two or more virtual markets are mediated by publish-subscribe systems. We consider a scaled down version of the CBB model, in which only three stages are operational, namely; *product identification* (by consumers) , *product and merchant brokering* (by

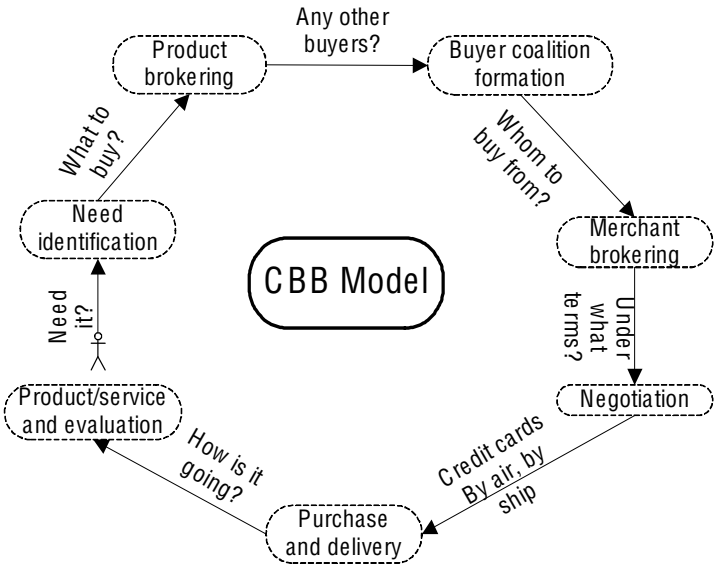


Fig. 4.1.: *Consumer Buying Behavior Model*

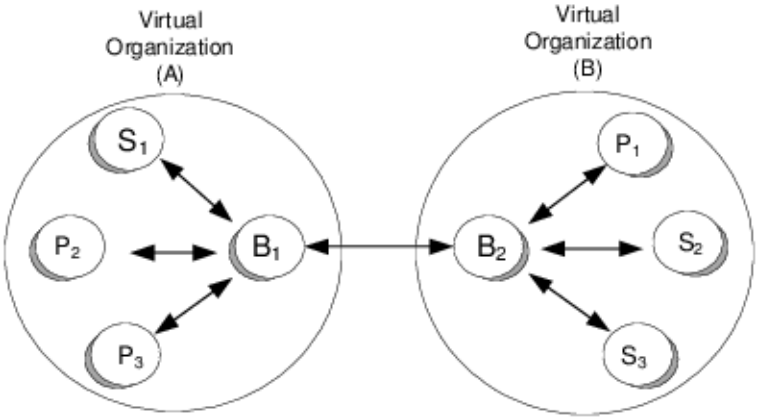


Fig. 4.2.: *Publish-Subscribe Mediated Market*

the Brokers); and suppliers (publishers) have to send in their products (publications) too. The other stages of the CBB model such as buyer coalition formation, negotiation, product delivery and evaluation are outside the scope of this chapter. Figure 4.2 presents a high-level overview for the virtual organization architecture under consideration. The organizational setup is mediated by Publish-Subscribe systems. The Brokers (B_1 and B_2) are responsible for aggregating subscriptions and publications from Subscribers (S_1, S_2 and S_3) and Publishers (P_1, P_2 and P_3) respectively. Virtual markets A and B collaborate on subscriptions and publications through Brokers B_1 and B_2. In case Subscriber S_1 is interested in a subscription that is not available in B_1, the request would be forwarded to B_2 by B_1. The presented scenario requires information to be handled and disseminated across virtual markets containing Subscribers and Publishers with diverse interests; some of which could be malicious towards some Publishers or subscribers.

4.2 Security requirements and assumptions

This chapter considers a scenario in which Subscribers and Publishers do not wish to reveal their identities to other participants in a publish-subscribe mediated system.

An environment in which Publishers, Subscribers and Brokers are interested in learning about transaction details of other parties is assumed. This implies that curious Brokers may want to know what Publishers and Subscribers are respectively selling and buying. Publishers may want to access information concerning transactions for particular Subscribers. Conversely, curious Subscribers could be interested in knowing identities of Publishers selling particular categories of products.

We consider three categories of security requirements, namely; confidentiality, privacy and integrity. These are further explained in the enumeration below.

i. ***Confidentiality***: This requirement applies to the objects which are being traded in the publish-subscribe mediated systems. Publications (offers) and Subscriptions (requests) are supposed to be kept secret from all participants in the environment

ii. ***Privacy***: This requirement applies to identities of Publishers and Subscribers. Publishers and Subscribers do not wish to have their identities revealed to any parties (i.e. Publishers, Subscribers and Mediators) in the environment.

iii. ***Integrity***: Messages and objects exchanged in the trading protocols are supposed to be protected from tampering by unauthorized entities.

Use-case scenarios for such requirements can be found in the stock market or job recruitment agencies. Considering an example of recruitment agencies, markets may desire their identities to be kept secret until subscribers or job applicants have sent their applications. Applicants may also desire their job searches to be kept private in the publish-subscribe system. There are various reasons for such requirements whose rationale is outside the scope of this research.

4.3 Related work

This section presents a review of solutions previously suggested in literature to provide for confidentiality, privacy and integrity requirements in publish-subscribe mediated environments. Their weaknesses are highlighted in this section and a new scheme to mitigate these weaknesses is presented in section 4.4.

4.3.1 Multi-layer encryption scheme

Shikfa et al. [62] suggested a technique for guaranteeing confidentiality and privacy in publish-subscribe networks by using commutative cryptography [63]. This scheme assumes that all the correspondents in the publish-subscribe environment have already received shared keys. The suggested scheme relies on the commutative property of the Pohlig-Hellman cryptosystem [64] to allow removal of encryption layers while preserving others in order to enforce data confidentiality. The encryption and decryption keys in the Pohlig-Hellman cryptosystems differ; thus having asymmetric properties. This cryptographic scheme requires that the encryption and decryption keys are kept secret since anyone can generate a second key with knowledge of either of the keys. Security of the cryptographic system depends on hardness of the discrete logarithmic problem.

The multi-layer encryption scheme suggested employs four security primitives, namely; (1) Encrypt-Filter: Used by subscribers to create filters. (2) Encrypt-Notification: Used by publishers to encrypt notifications. (3) Secure-Lookup: Used by Brokers to perform matching functions of filters to notifications. (4) Secure-Table-Building: Used by Brokers to build a routing table and compare encrypted subscriptions. The design of the four security primitives is based on commutativity properties of the Pohling-Hellman scheme. Brokers can add and suppress encryption layers on entries in the routing table and then remove some of them during lookup without accessing details of the subscriptions or publications.

There are several short-comings of secure routing with multi-layer encryption using a Pohlig-Hellman (commutative-homomorphic) scheme.

Firstly, is the key-distribution problem. Addition and removal of encryption layers depends on the participants respectively having the required encryption and decryption keys. This is a challenge for commutative cryptography where both (encryption and decryption) keys are required to be kept secret. Unfortunately, the Pohlig-Hellman scheme by design allows a second key to be generated with knowledge of one of the keys. If an adversary or curious brokers gains access to one of the keys they can generate the corresponding second key.

This challenge is assumed to be non-existent by Shikfa et al. [62]. We find this assumption impractical. Key distribution and secrecy of all keys cannot be ignored for practical deployment of such a system.

Secondly, Shikfa et al. [62] assume non-dynamic subscribers. This is clearly a problem, since an on-line system cannot be expected to have a static number of users. Consequently, assumptions concerning publishers having secret keys for

all available subscribers are highly flawed. The secrecy of keys in commutative cryptography requires a high degree of trust among entities possessing the keys of correspondents. Any accidental or malicious disclosure of one of the keys would lead to an absolute violation of all security requirements since corresponding keys can be generated from either of the encryption or decryption keys.

Lastly, practical deployment of cryptographic schemes requires implementation of the indistinguishability property so that a cryptanalyst may not gain useful information from a given cipher-text. This property when implemented in the scheme presented by Shikfa et al. [62], would make cipher-text comparisons absolutely impossible.

4.3.2 Secure publish-subscribe and matching schemes

Several schemes related to our work were previously reviewed in section 6 of [62]. These included *Secure Multi-Domain Systems*, *Event Notification Systems* [65], *Content-Based Infrastructures* [66], and *Fuzzy Private Matching* [67]. We encourage the reader to review section 6 of [62] for details of weaknesses and strengths for these schemes.

4.4 Proposed solution and system design

This section presents our suggestions for a solution to enforce privacy, confidentiality and integrity in publish-subscribe mediated virtual markets. The proposed solution is built on well established security techniques such as cryptographic hashes and public-key cryptography. Trusted Anonymizers (TA) are also used to facilitate processes required for enforcing security requirements specified in subsection 4.2. A principle for separation of privileges [68] is used to enforce subscriber and publisher privacy.

An overview of interactions between Brokers, Subscribers and Publishers was previously presented in figure 4.2 without details of security techniques deployed in the system. Figure 4.3 presents a new architecture for secure publish-subscribe mediated virtual markets by deploying Trusted Anonymizers (TAs) and Public-Key cryptography. The Trusted Anonymizers (TA_i) are used to enforce privacy requirements by acting as intermediaries for message exchanges between the Broker (B_l), Subscribers (S_j) and Publishers (P_k). The crossed arrow in figure 4.3 is an indicator that no direct interactions should happen between the two entities. The Brokers (B_l) should never communicate directly with the Publishers (P_k) or Subscribers (S_j).

This design is motivated by scenarios in which brokers that are acting as market enablers (information routers) may also have self interests in some of the transactions

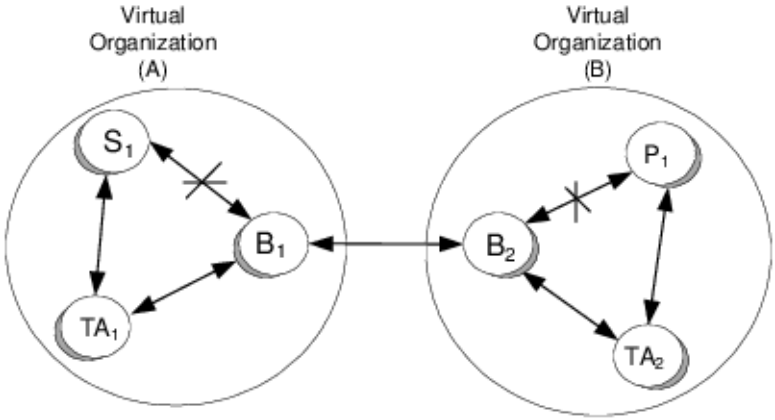


Fig. 4.3.: *Secure Publish-Subscribe Mediated Market*

taking place in the network. Such scenarios have been observed in agricultural markets for agricultural produce in Uganda and similar develping countries in sub-Saharan Africa.

It has been observed as indicated in subsection 2.2.2 that brokers act as aggregators for produce and could at any moment act as buyers or sellers themselves. In such circumstances, the privacy of buyer or sellers would be at risk. Having a Trusted Anonymizer whose role is primarily maintaining system security helps to separate privileges in the network.

The presence of Trusted Anonymizers is analogous to the presence of a Key Distribution Center (KDC) in the Kerberos [69] authentication protocol. The presence of Brokers in this application design is also analogous to exit-nodes in the TOR (anonymity network) network [70]. Brokers act as linkages for markets that are external to the current virtual organization.

Section 4.5 below presents details of the security protocol used to enforce confidentiality, privacy and integrity requirements for participating parties.

4.5 Security protocol

The TA is the only trusted element in the security protocol for this publish-subscribe mediated system. As previously indicated in the introduction section, security requirements are enforced using public-key cryptography and cryptographic hashes. The assumptions presented below are considered for the security protocol supporting secure interactions between the Publishers (P), Subscribers (S), Trusted Anonymizers (TA) and Brokers (B).

i. All participating entities can obtain verifiable public-keys for their correspondents. That is to say, a public-key server is available to all entities to obtain valid digitally signed keys.

ii. We also assume that the system inherits generic assumptions from public-key cryptography. Such assumptions include secret-key confidentiality.

iii. The scheme trusts that the TAs will not reveal routing information to adversaries. This implies that routing information collected by the TAs must be protected and their computations are assumed to take place on a trusted platform.

iv. The software executing on the Publishers' and Subscribers' terminals is assumed to be trusted. This software is responsible for generating the salt to be concatenated with the requests and offers. The process of concatenating a salt to the messages is strictly automated (achieved by software). Publishers and Subscribers cannot choose whether or not to concatenate a salt to their requests or offers. This operation is mandatory and is enforced through software on the Publishers and Subscribers terminals.

4.5.1 Publications

This subsection presents the component of the protocol for securely publishing content in the publish-subscribe system. In (4.1) and (4.2) formal components of the protocol are presented.

$$P_1 \rightarrow \mathrm{TA}_2 : [\mathrm{hash}(\mathrm{offer} \,||\, \mathrm{salt}) || \,\mathrm{TS}_1]_{\mathrm{KU}_{\mathrm{TA}_2}} \tag{4.1}$$

$$\mathrm{TA}_2 \rightarrow B_2 : [\mathrm{hashed\_offer} \,||\, \mathrm{TS}_2]_{\mathrm{KU}_{B_2}} \tag{4.2}$$

$$\text{Where } \mathrm{hashed\_offer} = \mathrm{hash}(\mathrm{offer} \,||\, \mathrm{salt})$$

TS_1 and TS_2 are timestamps which are supposed to be checked by the recipient in order to detect replay attacks. Furthermore, offers submitted by the publishers are sent as hashed values after concatenating them with a "salt". The concept of a salt being concatenated with the requests and offers is important for preventing dictionary attacks on hashes by either malicious Mediators or Trusted Anonymizers. The factors concerning the choice of ***hash functions*** and ***salt management scheme*** deserve much attention. The details of these choices are further discussed in subsection 4.5.4. This component of the security protocol achieves three objectives:

i. Privacy of the Publisher (P_1) is enforced by the Trusted Anonymizer (TA_2) eliminating direct interaction with a possibly curious Broker.

ii. Integrity of the messages is also enforced by encrypting messages using public-keys ($\mathrm{KU}_{\mathrm{TA}_2}$ and KU_{B_2})

iii. Message confidentiality is achieved by sending hashed offers to entities participating in the protocol.

4.5.2 Subscriptions

This subsection presents the component of the protocol for securely requesting for content from the publish-subscribe system by the Subscribers (S_j).

$$S_1 \rightarrow \mathrm{TA}_1 : [\mathrm{hash}(\mathrm{request} \,||\, \mathrm{salt}) || \,\mathrm{TS}_3]_{\mathrm{KU}_{\mathrm{TA}_1}} \tag{4.3}$$

$$\mathrm{TA}_1 \rightarrow B_1 : [\mathrm{hashed\_request} \,||\, \mathrm{TS}_4]_{\mathrm{KU}_{B_1}} \tag{4.4}$$

$$\text{Where } \mathrm{hashed\_request} = \mathrm{hash}(\mathrm{request} \,||\, \mathrm{salt})$$

Again this component of the security protocol is used to enforce privacy for the subscriber and to protect message confidentiality and integrity using principles similar to those presented in subsection 4.5.1 above.

4.5.3 Routing tables

The Trusted Anonymizers (TAs) and Brokers (Bs) are supposed to keep secured routing tables which would be used to identify correct destinations of responses or feedback for participants.

The routing tables (I and II) created by the TAs are used to match Publishers or Subscribers with their respective hashed offers or requests. In case Brokers send feedback to the TA concerning a request which can be served (i.e. a match has been found), the concerned TA has to search in the routing table for the subscriber corresponding to a stored hash request for feedback to be sent.

The routing tables created by the Brokers (Bs) are used to match TAs to the hashed requests or offers they forwarded so that a route for feedback can always be established when a match is found. The brokers use the routing table to identify a given TA_l that sent them a particular hashed request or offer. Table III shows a sample *Brokers' table of subscriptions*.

Publisher	Hash Value
P_1	$[\text{hash}(\text{offer} \,\|\|\, \text{salt})]_1$
P_2	$[\text{hash}(\text{offer} \,\|\|\, \text{salt})]_2$
P_3	$[\text{hash}(\text{offer} \,\|\|\, \text{salt})]_3$
...	...
P_i	$[\text{hash}(\text{offer} \,\|\|\, \text{salt})]_i$

Tab. 4.1.: TAs' table of Publications

Subscriber	Hash Value
S_1	$[\text{hash}(\text{request} \,\|\|\, \text{salt})]_1$
S_2	$[\text{hash}(\text{request} \,\|\|\, \text{salt})]_2$
S_3	$[\text{hash}(\text{request} \,\|\|\, \text{salt})]_3$
...	...
S_j	$[\text{hash}(\text{request} \,\|\|\, \text{salt})]_j$

Tab. 4.2.: TAs' table of Subscriptions

Likewise, the Broker has to store a table of publications which will be used to match TAs to corresponding requests from subscribers. Table IV is a sample *Broker routing table* for publications. After building Tables III and IV, Brokers B_1 and B_2 will possess hashed values of requests and offers received from Trusted Anonymizers. The presented sample tables do not have any optimization features such as indexing. This would of course be a relevant feature in a practical deployment. For example, tables III and IV could be combined by a Broker to create a match-making table consisting of a Primary-Key, Requesting-TA, Offering-TA and Hashed-Match columns.

The Brokers do not communicate directly with the Publishers and Subscribers, but they have the ability to perform matching functions between requests and offers received through the TAs. A ***request*** will be matched to an ***offer*** by a Broker if the hashes in protocol sessions (2) and (4) are equivalent. Whenever a Broker receives a hashed request from a TA, this hash is compared with contents of the publications table. In case a match is not found, the Broker (e.g. $B1$) would forward the request to another Broker (e.g. $B2$) for a match to be found.

After finding matching hashes, the Broker would then notify both the *"requesting"* TA_i and the *"offering"* TA_j about the success. The notification procedure is formally presented below.

$$B_1 \rightarrow \text{TA}_i : [\text{TA}_j \,||\, \text{hashed\_offer} \,||\, \text{TS}_5]_{\text{KU}_{\text{TA}_i}} \tag{4.5}$$

$$\text{Where } \text{hashed\_offer} = \text{hash}(\text{offer} \,||\, \text{salt})$$

Trusted Anonymizer	Hash Value
TA_1	$[\mathrm{hash}(\mathrm{request} \,\|\|\, \mathrm{salt})]_1$
TA_2	$[\mathrm{hash}(\mathrm{request} \,\|\|\, \mathrm{salt})]_2$
TA_3	$[\mathrm{hash}(\mathrm{request} \,\|\|\, \mathrm{salt})]_3$
...	...
TA_l	$[\mathrm{hash}(\mathrm{request} \,\|\|\, \mathrm{salt})]_l$

Tab. 4.3.: Brokers' table of Subscriptions

Trusted Anonymizer	Hash Value
TA_1	$[\mathrm{hash}(\mathrm{offer} \,\|\|\, \mathrm{salt})]_1$
TA_2	$[\mathrm{hash}(\mathrm{offer} \,\|\|\, \mathrm{salt})]_2$
TA_3	$[\mathrm{hash}(\mathrm{offer} \,\|\|\, \mathrm{salt})]_3$
...	...
TA_k	$[\mathrm{hash}(\mathrm{offer} \,\|\|\, \mathrm{salt})]_k$

Tab. 4.4.: Brokers' table of Publications

The message sent to the *"requesting"* TA_i consists of the identity of the *"offering"* TA_j, hashed value of the offer (obtained from the Broker's table of publications) and a timestamp to prevent replay attacks.

$$B_1 \rightarrow \mathrm{TA}_j : [\mathrm{TA}_i \,||\, \mathrm{hashed\_request} \,||\, \mathrm{TS}_6]_{\mathrm{KU}_{\mathrm{TA}_j}} \tag{4.6}$$

$$\text{Where } \mathrm{hashed\_request} = \mathrm{hash}(\mathrm{request} \,||\, \mathrm{salt})$$

Similarly, the message sent to the *"offering"* TA_j, consists of the identity of the *"requesting"* TA_i, hashed value of the request and a timestamp to prevent replay attacks. The *"offering"* TA_j then notifies the Publisher (P_i) about the demand for their offer as shown in the protocol session below.

$$\mathrm{TA}_j \rightarrow P_i : [\mathrm{hashed\_offer} \,||\, \mathrm{TS}_7]_{\mathrm{KU}_{P_i}} \tag{4.7}$$

$$\text{Where } \mathrm{hashed\_offer} = \mathrm{hash}(\mathrm{offer} \,||\, \mathrm{salt})$$

This part of the protocol also enforces the required security requirements of privacy, confidentiality and integrity for the publisher. The Broker will not be able to tell the identity of the Publisher, due to the indirect communication through a Trusted Anonymizer. Additionally, the TA_i also notifies the Subscriber (S_i) about the successful discovery of an offer to request.

$$\mathrm{TA}_i \rightarrow S_i : [\mathrm{hashed\_request} \,||\, \mathrm{TS}_8]_{\mathrm{KU}_{S_i}} \tag{4.8}$$

$$\text{Where } \text{hashed\_request} = \text{hash}(\text{request} \,||\, \text{salt})$$

Now the Subscriber is required to generate a new unsigned public-key which will be used to enforce confidentiality and integrity requirements for delivery of the required publication. Presented below is the last component of the protocol.

$$S_i \rightarrow \text{TA}_i : [\text{KU}^*_{S_i} \,||\, \text{TS}_9]_{\text{KU}_{\text{TA}_i}} \tag{4.9}$$

Here $\text{KU}^*_{S_i}$ is the new unsigned public-key to be shared with the Publisher.

$$\text{TA}_i \rightarrow P_i : [\text{KU}^*_{S_i} \,||\, \text{TS}_{10}]_{\text{KU}_{P_i}} \tag{4.10}$$

Now, the Publisher (P_i) has an unsigned public-key for the Subscriber (S_i) received through the Trusted Anonymizer (TA_i) and can encrypt messages which can only be retrieved by S_i.

$$P_i \rightarrow \text{TA}_i : [[\text{Object} \,||\, \text{TS}^*]_{\text{KU}^*_{S_i}} || \, \text{TS}_{11}]_{\text{KU}_{\text{TA}_i}} \tag{4.11}$$

Finally, S_i can receive the secret object encrypted by the new unsigned public-key after TA_i has removed encryption layer in protocol session (4.11).

$$TA_i \rightarrow S_i : [\text{Object} \,||TS^*]_{KU^*_{S_i}} \tag{4.12}$$

In the next section we present a discussion of issues surrounding cryptographic hashing functions and their implications to the overall security of the proposed protocol in a Publish-Subscribe Mediated System.

4.5.4 Properties of cryptographic hash functions

The guarantee of security requirements for the proposed system is highly dependent on the strengths of the cryptographic hash functions. The enumeration below presents key properties for hash functions previously suggested in literature [71]. These properties are a prerequisite for providing various security requirements to any system considering to use cryptographic hash functions:

i. Given a message (m) it should be easy to compute a hash value ($\text{hash}(m)$) from the message.

ii. Given $x = \text{hash}(m)$, it should be computationally infeasible to retrieve m from x.

iii. It is computationally difficult for an adversary to modify m without the $\text{hash}(m)$ changing.

iv. Given two messages (m_1 and m_2) where $m_1 \neq m_2$, it should be infeasible finding $\text{hash}(m_1) = \text{hash}(m_2)$.

Given the hash function properties above, the proposed scheme would always generate unique hash values for various offers and requests respectively submitted by the publishers and subscribers. Comparisons for equality between hash values for offers and request would also be possible since hash functions are deterministic and will always generate the same hash value for a particular input message.

If the hash function used in the system is poorly designed, then the hash values could be easily cracked by attackers. Hashing schemes such as MD5-crypt [72, 73, 74] and Bcrypt [75] use slow algorithms in-order to minimize the number of guesses which can be made by an attacker. Basically, the attacker would need much more time to crack a hash value with a slower algorithm as compared to other faster alternatives such as SHA-2 [76] family of hash functions. We are also aware of vigorous efforts for developing a more secure hash function (SHA-3) [77] conducted by the United States National Institute for Standards and Technology (NIST) (http://csrc.nist.gov/groups/ST/hash/sha-3/).

The guiding principles for creating and choosing the salt are further explained in the next subsection (4.5.5).

4.5.5 Choosing a salt

The main objective of concatenating a salt with the messages (offers and requests) is to minimize possibilities of successful dictionary attacks. Adversaries in the network, curious brokers, subscribers and publishers may want to run dictionary attacks on messages with the objective of compromising confidentiality and privacy requirements.

Concatenating a salt to messages would tremendously reduce possibilities of dictionary attacks on the hashed values. An attacker would not succeed in deriving the plain text message from comparisons of hashes with those from words in standard dictionaries. The random bits attached to the messages would make such attacks very difficult in terms of storage requirements and computation. The salt has to be kept secret from system participants and any-other external entities so that attackers have limited information for guessing messages corresponding to hashed values.

The salt to be concatenated with the request or offer has to be carefully chosen in the global environment of the system. This is important for feasibility of matches between hashes of requests and offers to be preserved. Implementing a scheme in

which randomized salts are appended to messages would definitely fail all comparisons between requests and offers.

It is important to note that the system software is responsible for generating a salt for the Publishers and Subscribers. This implies that users do not have control over the process of creating a salt. Equally, the timestamps appended to the messages are system generated and the system has to rely on a time server for synchronizing all clocks on participating nodes.

Salt protection

The software that generates and protects the salt from being revealed to buyers, sellers and brokers is part of the Trusted Computing Base (TCB)[78]. The TCB is an enforcer of security in an environment that is not trusted. An approach that has been widely successful in offering a Trusted Computed Base in untrusted environments is the deployment of Smartcards[79]. The costs for Smartcards is significantly low yet they offer a computing platform that can be used to securely generate a salt and also store it to prevent adversaries from tampering with it.

Smartcards are tamper evident: this implies that it would be possible to detect when an adversary tries to compromise it. Smartcards are also tamper proof to a large extent. Most modern smartcards are designed to be difficult to tamper with. The skill and operation cost of tampering with a modern Smartcard without destroying it and its content is very high and typically exceeds the gains anticipated from the target.

The next subsection (4.6) provides more details on considerations for formatting messages in the secure publish-subscribe system.

4.6 Message formatting

In order for comparisons in the system to make sense, message formats are supposed to be kept consistent. The format in which requests are concatenated with a salt and then encrypted, should be kept consistent with the subscriptions/offers.

This condition is particularly sensitive for the salt. If the salt concatenated with requests differs from that concatenated with the offers, then matching between offers and requests would be infeasible.

The global system environment is supposed to agree on a salt to be used for a particular period of time. It would be desirable to frequently change the salt to

minimize chances of successful guesses. Such correct guesses would also increase chances of successful dictionary attacks on exchanged messages. Furthermore, the salt has to be synchronized with the publishers and subscribers via a secure channel.

A poorly chosen salting mechanisms will either render the security schemes unusable due to computationally incompatible offers and requests or the hash values will get easily broken by a curious broker and consequently users' privacy broken.

Example matching with price information

In order to bring the comparison of offers into context, we consider a common problem of purchasing drugs for example for the treatment of HIV/AIDS. The purchase of these drugs by patients usually raises privacy needs most especially for individuals that do not want to have their identities revealed as HIV sufferers. Anti-Retroviral (ARV) drugs purchase example is shown below as an evaluation example.

$$\text{Publisher}_i \rightarrow \text{Market} : [\text{hash}(\text{offer}_i \,||\, \text{salt})||\, \text{Price\_of\_offer}_i]_{\text{KU}_{\text{Market}}} \tag{4.13}$$

An example seller submission would be $[\text{hash}(\text{arv\_drugs} \,||\, \text{salt})||50\,\text{euros}]_{\text{KU}_{\text{Market}}}$

$$\text{Publisher}_j \rightarrow \text{Market} : [\text{hash}(\text{offer}_j \,||\, \text{salt})||\, \text{Price\_of\_offer}_j]_{\text{KU}_{\text{Market}}} \tag{4.14}$$

Another example seller submission would be
$[\text{hash}(\text{arv\_drugs} \,||\, \text{salt})||52\,\text{euros}]_{\text{KU}_{\text{Market}}}$

$$\text{Buyer}_b \rightarrow \text{Market} : [\text{hash}(\text{request}_b \,||\, \text{salt})||\, \text{Price\_of\_offer}_b]_{\text{KU}_{\text{Market}}} \tag{4.15}$$

An example buyer request would be $[\text{hash}(\text{arv\_drugs} \,||\, \text{salt})||51\,\text{euros}]_{\text{KU}_{\text{Market}}}$

We can observe from the examples that $\text{hash}(\text{arv\_drugs} \,||\, \text{salt})$ is similar in all the three submissions and therefore a comparison is possible based on fourth hash property in subsection 4.5.4.

Since our privacy and confidentiality requirements are with the commodity being traded and identity protection, the price information does not need to be part of

the hashed value. Indeed adding price information to the hashed content would generate incomparable hashes since seller prices would typically differ.

4.7 Solution evaluation

This section discusses the weaknesses and strengths of the proposed scheme for providing confidentiality, integrity and privacy in publish-subscribe mediated virtual markets.

i. Confidentiality of the salt generated at the Publishers' and Subscriber's terminals is dependent on the trust in the software responsible for generating the salt. The Publishers and Subscribers should not be able to gain access to the salt. This implies that memory protection for the generated salt should be provided. The choice of programming language for implementing this software is critical for the security of the system. Requirements such as type-safety and memory protection should be guaranteed by the implementation. Various form of software vulnerabilities have previously been discussed in literature [80, 81].

ii. The Trusted Anonymizers (TAs) may turn against the Publishers and Subscribers to violate security requirements of privacy, confidentiality and integrity. The seemingly easy requirement to violate among those presented is privacy of Subscribers and Publishers by the TAs. The TAs are the first point of contact for the subscriber and publishers when they want to respectively buy and sell items via the Publish-Subscribe environment. It is practically infeasible to have message encryption without sharing keys TAs so that message confidentiality and integrity are preserved in the presence of an adversary in the environment.

iii. Attaching time bounds on validity of messages would not improve the security situation. Confidentiality and privacy can still be attacked using off-line techniques by a malicious Trusted Anonymizer. The broker has a chance to compromise message confidentiality when they copy the message and use available time and resources to learn about Subscriber and Publisher messages long after the transaction was completed.

iv. If the brokers succeed in cracking the hashes, they will not know the publisher of the item or in case of buying, they will not be able to tell who wishes to buy. However, successful off-line attacks by the TA would break both confidentiality and privacy of the message and Publisher-Subscriber respectively.

v. It is difficult to eliminate the compromise on hashing technique since we need to blind-match requests to offers. Encryption would have provided a solution less susceptible to off-line attacks, but it would render comparisons impossible.

4.8 Conclusions

The proposed scheme is rigid as far as message formatting is concerned. Messages should be created in a standardized format for all participants so that matching requirements can be consistently met.

Although it is not our objective to prevent the TAs from knowing details of requests and offers, the hashed messages make this implicit security objective possible. The TAs will know identities of participants but will not have access to message details.

Performance of hash functions is guaranteed to be faster than other deterministic cryptographic techniques such as homomorphic encryption schemes. The hash generation procedure is assumed not to impose a performance penalty on the system due to efficiency requirements for hash algorithms as stated in the enumeration of subsection 4.5.4. The generated hash-value is far easier to encrypt than the original message due to the significant size differences between a message and its fingerprint. This presents the benefit of fast encryption for the resultant light-weight content.

We have presented a scheme which offers a practical solution for confidentiality, privacy and integrity requirements in publish-subscribe mediated virtual markets. The compromises made (stated in section 4.7) are also practically sound for the target requirements.

5 An auction system for improved agricultural trade in developing countries

This chapter presents the need for developing an incentive compatible electronic market that efficiently connects trader agents in search of farmer agents with produce for sale and farmer agents in search of trader agents in need of produce to buy. To this end, this chapter envisages an auction market for agricultural trade that operates using a Short Messaging Service (SMS) interface. In this chapter, we consider the constraints for technology deployment in developing-world agricultural markets and conclude that neither of the existing approaches is sufficient. We argue instead for the introduction of a novel market mechanism better adapted to these constraints—particularly, to the need for interacting with the market via a basic (non-Internet-enabled) phone. In section 5.1 we present an introduction to electronic mechanisms for agricultural trade. In section 5.4 we present our proposed auction mechanism for agricultural trade and discuss the practical implementation of the auction market in section 5.5. Section 5.6 presents a discussion of the reputation system design and an evaluation of practical advantages of the auction design presented in section 5.7. Section 5.8 presents conclusions from our study.

5.1 Introduction

There have been recent attempts to use mobile and communications technologies to create agricultural advisory services, with a major focus on providing price information to farmers [3, 82, 83]. There have also been attempts to use phones and the Internet to set up markets in the developing world, usually based on classified advertisement listings or single-sided auction markets [84, 85, 82]. Several information systems have been implemented in form of agricultural advisory services in various developing countries [3]. The major goal of these technological implementations has been to help farmers in obtaining information for agricultural best practices to enhance their farm yields. The implemented advisory services have in most cases been used to provide farmers with access to market information. This

information dissemination process has helped farmers to gain incites into market trends to competitively price their produce.

The positive impact of agricultural advisory services has also been cast in doubt as reported in the evaluation by [86] which found a minimal impact on agricultural practices for farmers that were surveyed in 14 districts of cotton, onions and vegetable growing farmers in India. In 2005, Barrett et al., [1] presented a historical account of various transformations which had taken place in the agricultural markets of developing countries since the 1960s. Despite improvements in road networks, telecommunication infrastructure and free market conditions in most economies, some of the issues that impeded an efficient market place 50 years ago are still prevalent. Agricultural trade in developing countries is still based on informal contracts and market information largely shared by word-of-mouth. Trade networks among farmers and traders hardly grow beyond their historical social networks. Internet based e-commerce systems which have been ubiquitously adopted in the developed have not yet had a significant impact on agricultural trade in developing countries. Low bandwidth conditions, poor electricity infrastructure and high entry prices for computers have been significant hindrances to the adoption of Internet supported commerce.

Agricultural trade in developing countries makes a large contribution to the national Gross Domestic Product (GDP). Despite inefficiencies that were indicated in chapter 2, agriculture still employees more than half of the Ugandan population and a great deal of trade is conducted rurally. Uganda's agricultural sector for example contributes 24.4% ($12 billion) to GDP annually [5], is dominated by small-scale farmers. Agricultural markets in developing countries tend to be inefficient, due largely to poor information flow between buyers and sellers. Developing countries such as Uganda have experienced growth in their telecommunications infrastructure in recent years that have also been extended to rural areas. Within the last three years, new opportunities have been presented by the widespread adoption of mobile services such as mobile money transfer and by high mobile phone penetration.

The question as to why agricultural markets in Uganda are still inefficient remains unanswered. We argue in this this chapter that previous electronic market designs for agricultural markets have taken into consideration the incentives for a successful market design.

5.2 Obstacles to mobile-based trade

These qualitative and quantitative findings suggest that electronic markets would have much to offer participants in Uganda's agricultural market. However, such markets face many practical obstacles. Specifically:

- The costs of SMS messages pose a barrier to participation in mobile-phone-based auctions, particularly if a large number of SMS messages needs to be exchanged to conduct a trade. To put this argument into perspective, we analyze revenues for a farmer expecting to harvest 100 kilograms of maize grain. This farmer would expect a gross revenue of 50,000 UGX ($20 USD) given a conservative price of 500 UGX per kilogram of maize grain. Getting the grain ready to sell requires field maintenance over 6 months of growing the maize and approximately a month of drying the grain. Thus, the grain yields the farmer approximately 240 UGX (or about $0.10 USD) per day over these seven months. In contrast, the average rate for a single SMS message on Ugandan networks is 100 UGX ($0.04 USD).

- Traders are accustomed to physically examining goods before purchasing, claiming "seeing is believing." They may feel skepticism about whether a farmer will provide merchandise in the quality and quantities agreed upon electronically through a mobile-phone market system.

- Traders are accustomed to finding sellers through personal recommendations, and may be reluctant to trust a seller matched to them by an automated system. For example, we heard a concern from an urban trader that thieves might pose as sellers with cheap produce on a mobile market system in order to lure them to a remote location and rob them.

- Farmers may deliberately misinform traders about the quality and quantities of their products.

- Buyers who have committed to a farmer remotely may fail to arrive at the farmers' residences or markets to pay and take collection. Farmers are accustomed to immediate physical cash payments.

- Most farmers, traders and brokers are neither good writers nor readers. A complex SMS interface for participation in the trade would limit accessibility.

5.3 Market design considerations

This research work started with a proposal to implement an auction mechanism for agricultural trade. It was important that we designed a market mechanism met the following requirements;

- Minimize the number of message exchanges between users before a deal is concluded due to users' sensitivity to the costs of SMS messaging.
- Ability to represent commodity details such as species and quality in a single SMS message for listing on feature phones.
- Provide accountability in the system in form of a robust reputation mechanism for users not to misrepresent their market submissions.
- Provide an incentive compatible mechanism for buyers and sellers in the auction market.

A double auction mechanism [87] to facilitate trade using SMS messages on feature phones was considered for these requirements. The proposed design envisioned an auction mechanism in which farmers submit ask prices to the agricultural market for the produce they want to sell and traders also simultaneous submit bids for produce they wish to buy. The market would then match sellers with buyers that submitted a bid price above that of the sellers using a clearing price determined by the clearing algorithm. Parameters for setting the clearing price of the auction mechanism pose one of the major design challenges for the auction system.

5.3.1 Auction design structures

As presented in section 2.2, agricultural markets in Uganda are enabled by brokers and traders that buy produce from rural areas and transport it to urban markets. The market environment is assumed to involve three entities, namely; sellers (farmers), buyers (traders) and brokers who sometimes act as transaction advisors. We assume that transactions would be performed on a predefined list of commodities and geographical areas so that the SMS user interface is kept relatively simple. Traders, farmers and brokers would be given a printed list for them to learn codes for different districts in the country and commodities. In the listing below, we briefly present the roles that were initially thought to be played by each of the entities in the agricultural market and the information that would be needed for them to realize their objectives.

i. The farmers submit *ask prices* (*asks*) for which they would be willing to sell their produce in the market. These submissions are used to register a product type and capture the farmer's locations. Listed below is the information included in the traders' submissions:

   - *Product name and species*: Since the commodities being traded are agricultural products, farmers need to indicate the product name and or species.

   - The *quantity* available for sell from the farmer.

   - The *ask price* for the commodities.

ii. The brokers in the market are required to submit *price estimations* for the farmers' produce. This assignment is used on the assumption that brokers would perform unbiased evaluation of the farmers' produce. After each evaluation the broker would submit a quality indicative unit price for the produce to the market. This is necessary because traders and farmers currently do not have any discrete measures for quality at the farm level. Quality is evaluated over an informal continuous range or 'fair average quality' estimates. Price on the other side presents a value which implicitly includes quality evaluations. Given this price information a quality rating estimation for the produce can be obtained at the specified location using the demand-and-supply situations. The brokers would earn reputation points on good recommendations and lose points on inaccurate or poor evaluations. The information listed below is included in the broker's submissions:

   - Brokers would submit an estimate price (*product estimate price*) to the market for estimating produce quality.

   - *Farmer's location* from a well defined market reference point. The brokers provide distance information from a predefined trade location to the farmer's premises. The distance information is provided in terms of time required to travel to the farmer's location from the nearest trading center registered in the marker system. The usefulness of time is to distinguish between equal distances with different road conditions. Some rural seasonal roads are very poor during rain seasons and would have longer travel time than others.

iii. The traders also simultaneously submit their *bids* to the market for the products they wish to purchase. The information listed below is included in the trader's bids:

- The name of the product (*Product name*) that the trader wishes to buy.
- The *quantity* that the trader is bidding for.
- The unit price range (*minimum and maximum price*) for items to be purchased. This range of bid price is used by the bidding algorithm to place bids on behalf of the trader.
- $Maximum\ distance$ that the trader is willing to travel from the primary rural trading point. This distance measure would be used to compute bid prices for an distance between the best location and worst case distance locations.

At the time of registration, the trader would indicate their preferences for trading locations they would be willing to visit. These preferences would also be used to deliver message alerts for new offers in the market. The traders can also update these preferences by sending an SMS to the market system.

iv. Support for negotiation: Traders are highly accustomed to negotiation in the current trade environment. It is important for the proposed system to provide room for negotiation in order to achieve wide acceptance by stakeholders. After successful matching between the seller (farmer) and the buyer (trader) using a clearing price (p), the farmer and trader are notified. The trader is given a time frame to accept or reject the offer. If the offer is accepted by the trader, this implicitly implies that the trader and broker can enter into a negotiation for the final price above the ask price and below the bid price.

v. It is also further observed that numeric representation of reputation scores would not be very informative for the target group. We need to represent reputation in a meaningful style which can be easily communicated to the traders, brokers and farmers. It is important for all parties to have a clear understanding of the reputation feedback. We propose a scheme that is represented in a natural language. Essentially, a range of reputation scores in figures would be matched to a natural language range. Examples of such ranges includes; Platinum , Gold, Silver, Bronze and newbie ratings for traders and farmers. Since broker activities are mostly about trust, their scores could be; Exceptionally trusted, highly trusted, trusted, lowly trusted and untrusted.

5.3.2 Filtering rules

Due to the constraints of communication because of messaging costs, market interactions are required to be restricted to individuals with a high probability of actuating

the trade. Listed below are some of the filtering conditions for traders' and farmers' submissions. The traders could place bids that are filtered by:

- The minimum reputation level of the broker or farmer they would be willing to trade with, or restrict only to a list of "trusted" participants. Traders and farmers would earn reputation points on successfully completed transactions and would lose points on those where either sides is not satisfied by the transaction outcomes.

- The maximum distance of the farmer from the trader's primary trade location. This is important because traders care about transportation costs involved in collecting the produce.

- The minimum quality levels of produce that traders are willing to buy from farmers. The quality information about the produce would have to be vouched for by brokers.

The conditions listed below are proposed for optional broker involvement so that the market stays adaptive while also promoting accountability:

- We envisaged situations in which brokers may not be available to verify information from farmers about their produce. Such situations would call for a design in which the market system waits for feedback for a specific amount of time, after which the offers are forwarded for possible bidders. A time threshold would be set based on the nature of the product. If it is vegetables with a short storage span, then notifications would be released in no more than 3 hours. For products such as dry beans or maize, the waiting time can be allowed to be longer.

- In case the amount of money involved in a transaction is small, then the requirement of a broker would need to be relaxed. A threshold would be set for an approximate value of the product being submitted for auction. Since brokers are supposed to earn commissions from transactions on which they give feedback, transactions involving low priced commodities are likely not to be profitable in case brokers are required to perform quality checks.

- In case the trust level for the seller is high and above a specified threshold, such offers might be exempted from quality evaluations by brokers. The trust that the market places in any individual is defined by a reputation score which grows as a result of positive market activities and is reduced when something undesirable takes place. We are also mindful of scenarios in which some buyers and sellers might use their high reputation scores to act dishonestly because the market places a high trust in them. This issue presents temptations

of brokers submitting reviews without actually checking the produce. Since farmers also get notification messages about these ratings, it might be possible that complains would be raised by the farmer that their merchandise was rated without a physical inspection. In such cases the broker's reputation would be reduced by an amount that substantially reflects dishonesty and impacts their reputation.

Since the market needs to ensure reliability and accountability, the following conditions were proposed in order for this goal to be met: Presented in the listing below are conditions in which broker reviews are mandatory.

- When the approximate price of merchandise is above a specific threshold, then the market would require a quality verification by the broker. In this case the broker would contribute to the reliability attribute of the transaction.

- In circumstances where the farmer cannot be trusted, because of a low reputation score, then the market would require the broker to verify the information that was submitted by the farmer.

- We also consider scenarios in which the buyer explicitly indicates that they need a broker to verify the merchandise before committing to the purchase.

5.3.3 Auction interaction protocol

In this subsection we present our initial double auction protocol design for message exchanges in the proposed agricultural market systems.

i. We start is one part of the auction in which farmers submit products to the market. These products are grouped into commodities depending on their category or species and location. Presented in the session below is a structure of a message from the farmer to the market system.

$$F \rightarrow M : (Product\_Species, Quantity, \\ Village\_name, Ask\_price) \tag{5.1}$$

The *product name* in the message describes the product; for example beans, and the *species* provides more information about the quality of the product. The quantity is used to obtain a unit price from the *Ask_price* which will make it possible to defined normalized values for comparison purposes. The *Location_ID* is obtained from a list of predefined locations that have been submitted to the farmers, traders and brokers. We further need to obtain the *Village_name* since the predefined locations are likely to be within a radius of 10kms from the farmers' actual locations.

ii. After a farmer has submitted their produce to the market, a broker nearest to them is sent a request specified below to go and verify the produce.

$$M \rightarrow B : (Trans\_ID, Farmer\_ID, Location\_ID, \\ Village\_name, Farmer\_mobile\_number) \tag{5.2}$$

The transaction identifier (*Trans_ID*) is used to distinguish between commodities submitted by the same farmer. The mobile number of the farmer is important for the broker to obtain additional information for directions to the farmer's location. The village name also contributes to the accuracy of information to the farmer's location. The *Farmer_ID* is used by the market system when registering reports from brokers concerning the visited farmers. The broker is given *one minute* to accept or reject the request. If the broker rejects the request, two additional brokers are contacted. When they all decline to review the produce, the commodity is listed with the status *unreviewed*.

iii. The message below would be sent by the broker to the market after reviewing the farmer's produce.

$$B \rightarrow M : (Trans\_ID, < OKAY | NOT\ OKAY > Location\_ID, \\ Estimate\_travel\_time) \tag{5.3}$$

In the message above, the broker quotes the transaction identifier for a particular farmer's submission. The location identifier for the farmer is confirmed by the broker using the *Location_ID*. The estimated time (*Estimate_travel_time*) required to travel from the registered location identifier to the farmer's location is also received from the broker. The estimated price *Estimate_price* for the farmer's produce is used to compute the quality rating of the produce. This value is a unit price for the farmer's produce which is used to estimate the quality rating of the produce. The brokers are expected to be honest in their submissions and failure to do so would lead to loss of reputation points.

iv. Presented here is a scheme for computing the quality for produce submitted by the farmer. We note that the prices of produce in the country would differ due to differences in demand and supply conditions. The prices of produce can be mapped onto a quality scale between 1 and 10 using the lowest and highest prices from a given predefined trading zone. Given a location (A) with Min_{P_A} and Max_{P_A} as respectively minimum and maximum prices for a given product P ($Prod_P$). We can obtain the price for each unit scale of quality ($Quality\_unit\_price_{P_A}$) for $Prod_P$ using the equation below:

$$Quality\_unit\_price_{P_A} = \frac{(Max_{P_A} - Min_{P_A})}{10} \tag{5.4}$$

Given a broker estimate price ($Estimate\_Price_{P_A}$), we can calculate the quality rating for the farmer's produce at location A ($Quality\_rating_{P_A}$) using the equation below:

$$Quality\_rating_{P_A} = \frac{(Estimate\_Price_{P_A} - Min_{P_A})}{Quality\_Unit\_Price_{P_A}} \tag{5.5}$$

Using equation 5.4 we can obtain the quality rating for a product

v. Given that the market has received detailed information concerning the farmer's produce, it is now possible to classify these submissions into commodities. The records required for defining commodities are *Product name or species, Location_ID, Quality and Ask_price*

vi. Presented below is the message that is expected from the traders as they place their bids in the market. It deserves mention that the trader's asks are simultaneously submitted to the market with the farmers' bids.

$$T \rightarrow M : (Product\_name\ or\ species, Bid\_amount, Location\_IDs, FILTERS) \tag{5.6}$$

The $FILTERS$ might include the following options: Max_time, $Min\_quality$ and $Min\_broker\_reputation$.

The market would then match the trader's request using the bid price and any filtering options specified by the trader, for example during registration or bid submission. The location identifiers indicate the places that the trader would be willing to travel to buy produce. The maximum distance (Max_time) indicates the maximum time that a trader would be willing to travel from the specified trade locations preferences to the farmer locations.

vii. Presented below are details for the bidding algorithm to construct a bid on behalf of the trader. We assume that the minimum reputation for the broker as R_{min} and the maximum time the trader is willing to travel as T_{max}. For any given commodity in the market, we consider it to have the following attributes relative to a trader's preferences:

- The reputation (R) for the broker that vouched for the produce in the market system, where $R \in \{1, \ldots, 100\}$ and
- The time (T) required to travel from one of the trader's specified locations to the farmer's location where $T \in \{0, \ldots, T_{max}\}$.

The function for the trader's bid *per unit quantity* would follow as shown below:

$$Bid(R,T) = (Bid\_amount) \cdot \left(\frac{R-R_{min}}{100-R_{min}}\right) \cdot \left(\frac{T_{max}-T}{T_{max}}\right) \tag{5.7}$$

Using equation 5.7 we can determine the final bid amount (bid_amount) for the trader.

The condition $min\_price \leq Bid(Q,R,T) \leq max\_price$ should be satisfied by all bids submitted on the trader's behalf.

viii. After the market has computed the bid price on behalf of the trader, the final purchase price (Clearing_price) is communicated back to the trader after finding a match. The message below shows the feedback contents:

$$M \rightarrow T : (MATCH\_FOUND, Product\_name, Clearing\_price, Location\_IDs, travel\_time) \tag{5.8}$$

The message to the trader contains the village name ($village\_name$) in which the farmer is located and the travel time ($travel\_time$) required to the village from a well know reference point (defined by a $Location\_ID$).

ix. After receipt of this message the trader is supposed to either accept or reject the offer.

$$T \rightarrow M : (< ACCEPT | REJECT >) \tag{5.9}$$

x. After the trader has accepted the offer, the farmer is also notified that their ask has been accepted. The farmer is supposed to make final confirmation for availability of the produce by sending an $ACCEPT$ or $REJECT$ acknowledgement.

$$M \rightarrow F : (MATCH\_FOUND, Clearing\_price) \tag{5.10}$$

The farmer has the final choice to accept or reject.

$$F \rightarrow M : (< ACCEPT | REJECT >) \tag{5.11}$$

When both the farmer and trader accept, the product is put off the market and consider to have been sold. Transaction is expected to be completed by a trader physically visiting the farmer and making payments. After such a visit trader and farmer are expected to rate each others performance in the given transaction.

The next subsection presents design goals for the reputation system which is integrated into the market design in order to establish trust mechanisms between farmers, traders and brokers.

5.3.4 Service subscriptions

The service subscription phase provides provisions for market participants to update their subscription preferences. The major items for the participants to update are their product preferences. It is also required that group members are informed about these updates. This would act like a social network status update that will promote future interests among closely linked trade partners.

The protocol requires a *personal secret* challenge for individual subscriptions. The personal secret is used to prevent automated subscriptions from malicious elements that might wish to launch denial of service attacks. A nuisance or denial of service attack would be successful if participants are subscribed to a large number of products for which they have little or no interest. The service subscription and update protocol follows the same arrangement for brokers, farmers and traders. The term $Participant$ is used here to refer to traders, brokers or farmers.

The protocol for service subscriptions and updates follows the example protocol below:

i. Message request to add an item or product to a participant's interest list.

$$Participant \rightarrow M : [Add(Item_{Description})||Personal_{Secret}] \tag{5.12}$$

ii. Message request to remove an item or product to a participant's preference list.

$$Participant \rightarrow M : [Remove(Item_{Description})||Personal_{Secret}] \tag{5.13}$$

5.4 Proposed auction mechanism for agricultural trade in Uganda

We now describe our design of an auction mechanism to support SMS-based trading of agricultural commodities in developing countries. We propose a double auction market (see, e.g., [87]) in which buyers and sellers submit binding bids asynchronously, and the system periodically clears the market, matching compatible buyers and sellers and setting prices that are agreeable to both.

Algorithm 1: Assignment of asks and bids

Input: A set of Asks ($\mathcal{A} = \{\theta_1, \ldots, \theta_n\}$) and a set of Bids ($\mathcal{B} = \{\lambda_1, \ldots, \lambda_n\}$)
Output: A set $\mathcal{M}$ containing tuples (λ_j, θ_i) for matches between various bids and asks

$\mathcal{M} \leftarrow \emptyset$;
for $\lambda_j \in \mathcal{B}$ **do**
  $\mathcal{A}_j \leftarrow \emptyset$;
  `/* Find all feasible asks */`
  for $\theta_i \in \mathcal{A}$ *in decreasing order of* q_i **do**
    if $(c_j = c_i) \wedge (l_i \in L_j)$ & $(a_i \leq b_j)$ **then**
      $\mathcal{A}_j \leftarrow \{\mathcal{A}_j \cup \theta_i\}$
  `/* Keep only Pareto-optimal asks */`
  for $\theta_i \in \mathcal{A}_j$ **do**
    for $\theta_k \in \mathcal{A}_j$ **do**
      if $a_k \geq a_i \wedge d(l_j, l_k) \geq d(l_j, l_i) \wedge (a_k > a_i \vee d(l_j, l_k) > d(l_j, l_i))$ **then**
        $\mathcal{A}_j \leftarrow \mathcal{A}_j \setminus \theta_k$
  `/* Select ask with largest quantity */`
  find θ_l s.t $q_l \geq q_i \; \forall \; \theta_i \in \mathcal{A}_j \setminus \theta_l$;
  $\mathcal{M} \leftarrow \mathcal{M} \cup (\lambda_j, \theta_l)$;
  $\mathcal{A} \leftarrow \mathcal{A} \setminus \theta_l$

We assume a set of buyers B, a set of sellers S, and a set of mutually exclusive locations L. We represent the distance between any two locations using a function $d : L^2 \rightarrow \mathbb{R}$. C is a set of commodity types to be traded. An **ask** is a tuple $\theta_i = (l_i, c_i, q_i, a_i)$, specifying that seller located at $l_i \in L$ has $q_i \in \mathbb{N}$ units of commodity $c_i \in C$ that they are willing to sell at $a_i \in \mathbb{R}_+$ per unit. A **bid** is a tuple $\lambda_j = (l_j, c_j, q_j, b_j, L_j)$, specifying that a buyer located at l_j is willing to pay up to b_j per unit for q_j units of commodity c_j in any location within $L_j \subset L$. A bid θ_i and an ask λ_j are **feasible** iff $c_i = c_j$, $l_i \in L_j$ and $a_i \leq b_j$.

The goal of the market mechanism is to find a matching among the feasible pairs. Whenever a bid and ask are matched, we set the price to be the same as the ask price. We consider the fact that buyers prefer geographically closer asks, although we do not know exactly how much each buyer values a given reduction in distance. We propose a greedy algorithm to perform matches, which cycles through the bids, offering time-limited matches to buyers that are Pareto optimal with respect to distance and price. Specifically, we consider bids in the order received, and iterate through the following steps (explained more formally as Algorithm 1):

i. For the next unmatched bid λ_j, calculate the set of feasible asks A_j.

ii. Discard all asks from A_j that have been offered to another buyer.

iii. Further discard all asks from A_j that are not on the Pareto frontier trading off between distance and price. (That is, we discard each $\theta_i \in A_j$ for which there exists another $\theta_k \in A_j$ such that $a_k \leq a_i$, $d(l_j, l_k) \leq d(l_j, l_i)$, and either $a_k < a_i$ or $d(l_j, l_k) < d(l_j, l_i)$.)

iv. If A_j is nonempty, choose the $a_j \in A_j$ for which q_j is greatest and make a time-limited offer to the buyer who submitted the bid λ_j. Mark that ask as being under offer.

v. If any offers have been accepted by buyers, match the corresponding bid and ask. If any offers have expired or are rejected by buyers, mark them as not under offer and delete the corresponding bids and asks as feasible pairs.

vi. If any feasible pairs remain, return to step 1.

We note that this greedy clearing algorithm could be replaced with one that optimizes the quality of the matching using (e.g.) a mixed-integer programming formulation. However, observe that we face an online optimization problem: the rejection of a match by either party requires us to rematch the corresponding ask and bid. Because we do not know which matches will be rejected, it is therefore impossible for us to clear the whole market in a single, offline step. In ongoing work we are investigating whether we can improve market outcomes by leveraging more powerful clearing algorithms, and if so, whether these improved outcomes justify the increased computational cost of clearing.

5.5 Practical implementation of the auction market

We implemented an auction system based on the above mechanism, offering users both SMS and web interfaces. The SMS interface is accessed using a 4 digit short-code that is easy for users to remember, and is available in three languages: English, Luganda and Luo. Since most users in Uganda and other developing countries use low-end mobile devices, SMS is the main form of interaction with the system.

We also implemented a web interface, with the aim of facilitating more complex transactions for bulk buyers and sellers. Unlike the SMS interface where buyers and sellers are presented with a single dominant match on the Pareto frontier to accept or reject, the web interface presents a list of candidate matches.

Finally, we provide a helpline number with all SMS communications, which helps users who are unable to manage either of the above to verbally communicate their bids and asks. In practice we have also found it necessary to call back users who send unintelligible SMS messages.

The matching process occurs once per day. The matched asks to a bid are reserved for a specific period and during this time, those asks are not available for matching with any other bid. When the waiting period expires without the buyer accepting or rejecting, the asks are put back to a pool of available asks. While traders are asked to acknowledge acceptance or rejection of matches, we found that not all did so; knowing which matches have been accepted by both parties has therefore posed something of a challenge. We addressed this issue by matching a particular ask only a certain number of times, and assume thereafter that it has either been accepted or should be expired.

In addition to pages for buying and selling, our web interface offers a price discovery page for users to obtain price information based on locations in the country for a specified past number of days. Locations in the Ugandan setting have been defined to the level of parishes (the smallest administrative region in Uganda, with 6254 parishes in the country). This gives a high precision for location based price discovery services. More specifically, we defined each location as the centroid of a parish, and calculate $d(l_i, l_j)$ as Euclidean distance from this point.

When a new user sends any message to the system, they are first asked to provide their home parish. Following this registration step, the SMS interaction between farmers, traders and the market is keyword based and is structured as described in the following sections.

5.5.1 Farmer Asks

Farmers submit their asks to the market using a SELL keyword in their SMS message sent to 8228. An example SMS to sell 4500 kilograms of beans at UGX 900 would be defined in an ask SMS as follows; “SELL BEANS 4500 900”. The farmer would receive an acknowledgement with an Ask ID that can be used for follow-up inquiries. Note that farmers are not required to include their location information since this information is already part of their profile.

During buying and selling there is no attempt to differentiate the quality of produce on offer; we ask farmers and traders to assume ‘fair-average-quality’ (normally produce that is not cleanly sorted or graded). This allowed us to keep the format of the SMS message simple. Buyers are able to inspect produce and renegotiate if necessary before making final payments.

5.5.2 Trader Bids

The trader bid submission follows an SMS syntax similar to that of farmers, except that the keyword changes to BUY. A trader who wishes to purchase 5000 kilograms of beans at UGX 800 would send the message "BUY BEANS 5000 800". Such a bid will attract a possibility of matches for beans across all locations in the country. Traders can optionally include location filters so that their bid matches with asks are restricted to a particular location. Such a message will be constructed as follows; "BUY [PRODUCE] [QUANTITY] [UNIT PRICE] [LOCATION]". Bids can be made on regions (5 across the country), districts (112) or parishes (6254).

5.5.3 Market Matches

Market matches are made using the double auction mechanism described above. Matches are not permitted if either trader blacklisted the other. Buyers are given a set of candidate offers along the Pareto frontier trading off price and distance. The accept or reject request contains the clearing price and location of the seller. Buyers are expected to respond in an SMS quoting the ID of the match. The syntax for an ACCEPT or REJECT SMS is "ACCEPT | REJECT [MATCH ID]". The match ID is typically a system-generated integer. The implementation ensures that buyers can only reject matches that belong to them; other REJECT or ACCEPT requests are ignored. The request to accept or reject is time limited; if the buyer does not respond after the specified period, then the match is removed and placed back to the pool of available asks. The same happens when a buyer rejects the offer. As noted above, however, this functionality was rarely used in practice, and so we set a limit on the number of times a particular ask can be matched.

5.5.4 Price discovery

Since this is an auction system where users do not know ahead of time what typical buying and selling prices will be, the system provides an SMS interface for users to learn produce price information. The price discovery specification is similar to that of the web interface. The SMS interface uses the PRICE keyword and the syntax is as follows; "PRICE [PRODUCE] [LOCATION] [NUMBER of DAY]". In this syntax, location and number of days are optional. The user can simply send "PRICE [PRODUCE]" and they will receive price information for a given produce for the past 7 days in Uganda. If location and time parameters are specified, then price discovery will only provide price information for a particular location for the requested number of days.

5.5.5 User registration

The registration phase is the first point of interaction between farmers, traders and the market system. A market registration process is expected to ensure that fake users (sybils) do not register on the system. Sybils are of particular concern for an electronic system since adversaries might automate this process and flood the system with invalid users. Such users would typically be used to submit fake reputation scores to their owners or accomplices. Users registrations are captured using the following syntax; "REGISTER [PARISH] [DISTRICT]". The parish and district elements are optional since we can obtain this information later on using callbacks to newly registered users.

5.6 Reputation system design

In an environment where the traders are not certain that farmers will deliver the promised goods and farmers being uncertain about the traders making payments to the prepared merchandise, a reputation system is employed to provide an opinion on trustworthiness of the involved parties. Farmers and traders may want to minimize risks of trade by restricting their business transactions to only reputable parties in the market. A reputation system that implements mechanisms for collecting information concerning behavior of farmers, brokers and traders in the market would deter moral hazards [88]. Reputation systems have been used in e-commerce systems to provide a record of past behavior for individuals and organizations. Such information is used as a basis for predicting behavior of entities before interacting with them. Reputation systems have played a deterrent role for unscrupulous behavior in online systems. A historical record of user actions and interactions acts as a reminder for actors to behave responsibly in the trade environment[89]. In addition to deterring bad behavior, reputation system also help consumers of various electronic services in the decision making process[90]. Individuals could be saved time for analyzing large amounts of information in order to form an opinion about an online service or product. A review of recommendation information about an individual or product is usually expected to give a satisfactory overview to support the decision making process. Reputation systems provide a means for consumers to analyze trust metrics [91, 92] normally represented as reputation scores collected from the network of interconnected participants. The design of a reputation system in the mobile-phone based market is aimed at creating a trust environment through which users can determine entities to trade with. The network of traders, farmers and brokers is thus expected to be self monitoring as actions by all actors are expected to be directly reflected in their reputation scores.

Dellarocas [88] previous presented the signaling and sanctioning roles of reputation mechanisms to respectively alleviate ***adverse-selection*** and moral-hazards in transactions. Adverse-selection refers to situations in which a lack of trust in the seller by consumers causes them to always offer low prices for goods and services. Typically such market habits could eliminate providers of high quality goods, since the lower quality providers are happy with the price offers from consumers. Signaling in such cases provides consumers with a tool or information to judge the quality of a product or service [93]. On the other hand ***moral-hazards*** occur when participants in a transaction do not act honestly. In the agricultural market, for example, farmers may not deliver the promised quality of goods after receiving payments from traders.

5.6.1 Reputation system design goals

The main objective of the reputation system proposed in this paper is to offer trust management between the farmers, traders, brokers and the market. Enumerated below are the specific goals to be achieved by the design of a reputation system for a mobile-phone based trading system.

i. The reputation system is expected to aid farmers in establishing trust levels between them and the traders before committing to any given transaction terms. Given bids between two competing traders, a farmer should find it compelling to offer a good deal to a trader with a higher reputation score. In so doing, traders that fail to get good deals from the farmers would also work to improve on their reputations scores through good behavior in the trade environment.

ii. To encourage brokers to submit genuine reviews concerning farmers' products under their review. Since brokers are responsible for informing the market about availability of new trade opportunities. It is important that their reviews can be trusted by other participants in the trade environment. A highly reputable broker would have their recommended products showing up among the favorites in the trade system. This arrangement is expected to promote truthful reporting by the brokers in order increase value for their future recommendations.

iii. Farmers to be truthful about their products. A successful trade indicated by satisfaction of the trader would lead to an increment in reputation points. The broker that vouched for a successful trade would also earn reputation points. The reputation scores for individual farmers would also be reflected in the farmer groups such that their cooperatives would know the people uplifting them and those letting them down. This social network is expected to provide a self monitoring mechanism amongst farmers, traders and brokers.

iv. Traders to abide by their commitments: Failure by traders to fulfill their agreements should lead to a reduction in reputation scores of the individual and the trader group to which they belong. The trader group would then provide peer pressure for the members to act responsibly.

v. The reputation system should provide traders and farmers a platform for reliable evaluation of risks or utility involved in dealing with various parties in the market. Reputation scores of individual farmers and their groups should aid traders in making decisions of trading amongst farmers in the market.

vi. New entrants in the market should not be heavily punished for having little or no reputation information. Additionally, the reputation score for a new entrant should not rival with those of longterm participants. This objective is intended to promote loyalty from existing system users as well as encouraging new participants.

vii. The system should preserve confidentiality of reputation score submissions to protect contributors from retaliation against each other. Some farmers, traders and brokers may retaliate towards other participants in-case they get to know individuals or groups that awarded them low scores.

5.6.2 Blacklisting reputation mechanism

We propose a blacklisting mechanism to manage reputation in the market systems. If buyers or sellers have a negative experience of dealing with somebody they have been matched with, they are encouraged to blacklist that user by sending a message of the form “BLOCK [PHONE NUMBER]”. This results in that buyer and seller never being matched again, and provides important information about the reliability of users.

The number of ’blacklistings’ received by a market participant would affect their future participation in market transactions. Good offers from reputable sellers or buyers would not be matched with users with a low reputation score.

5.7 Practical advantages of the auction design

We now discuss why this auction design is well suited to the constraints of developing-world agricultural commodity trading identified earlier.

- First, the sealed-bid, double auction mechanism requires very little communication between traders and the market. Each user has only to submit their bid

or ask, and (in the case of buyers) to respond to individual offers. SMS costs are therefore kept low.

- The process for dealing with location is necessary because it would be quite complicated for a buyer to specify the price they would be happy with at several distances from their home market, which might involve factors such as vehicles available to the buyer, road condition, and so on. A simpler alternative is to offer buyers a small number of Pareto optimal matches, and let them choose their preferred trade-off themselves. The ability to specify simple bids covering large areas is necessary in order to make offers to buyers outside their accustomed trading areas, thus avoiding a fragmented market.

- We note that once a price is proposed to both buyer and seller, it can be advantageous to allow them to negotiate further at the point of collection. It is important for the proposed system to provide room for negotiation in order to achieve wide acceptance by users, particularly as a mobile market system has the problem of not being able to specify in detail the quality of a product as accurately as a buyer would be accustomed to in face-to-face dealing. Indeed, this explains why our system does not allow for the specification of produce quality. (We note that produce of different qualities could in principle be represented as different commodities, in which case we could extend our definition of feasibility, since bids should be matchable to asks where the produce is either of the quality specified or higher.) Instead, we quote all prices for a baseline quality level, and allow traders to negotiate after a match has been made in the event that quality falls above or below this baseline.

5.7.1 Incentives for truthful bidding

Our auction mechanism offers buyers the dominant strategy of bidding truthfully. Thus, they do not need to reason about each other's bids in order to maximize their utility.

To back up this claim, we introduce notion for bidder utilities. Let v_j be the price at which the buyer expects to resell the produce in the market, and v_i be the cost incurred by the farmer to grow and harvest the produce. A buyer j's utility for trading at clearing price p is then $u_j = v_j - p$; a seller i's utility is $u_i = p - v_i$. Our mechanism always sets the clearing price to the seller's ask price a_i, and matches a buyer with a seller whenever the buyer's bid weakly exceeds the ask price ($b_j \geq a_i$). A bid is truthful if $b_j = v_j$.

Proposition 5.1
Buyers who want to trade only with a single seller have the dominant strategy of bidding truthfully under our double-auction protocol.

Proof 5.1 The result follows directly from the fact that truthful bidding is a dominant strategy in second-price auctions; nevertheless, because the proof is simple, we reproduce it here. If a buyer bids some amount $b_j > v_j$, he would either fail to get matched (obtaining utility 0) or get matched to items whose ask price $a_i \leq b_j$, being required to pay the ask price a_i. If $a_i \leq v_j$, the outcome is the same as under truthful bidding, and so the buyer might as well have bid truthfully. If $a_i > v_j$, the buyer pays more than he thinks the goods are worth, implying that he would have preferred not to trade. Similarly, if a buyer bids $b_j < v_j$, he would either receive the same match as before—meaning that he might as well have bid truthfully—or he would fail to be matched at a price $a_j < v_j$ at which he would have profited.

Observe that this result does not hold if buyers want to trade with many sellers and have complex preferences that cannot be expressed in our bidding language; e.g., nonlinear preferences over bundles of goods, such as a desire to buy enough produce to completely fill a truck, but no desire for produce beyond this amount. Even in this case, second-price bidding simplifies the strategic problem for buyers, albeit leaving sellers to their own devices.

We designed our market to favor buyers because our interviews made it clear that sellers (farmers) are much more desperate to trade, meaning that they are most interested in seeing more trades occur. Buyers also tend to be much more sophisticated traders, making them more likely to manipulate the system with untruthful bids if not offered dominant strategies. One might hope that dominant strategies could be offered to traders on both sides of the market; unfortunately, this is impossible in any efficient market that does not operate at an (unbounded) loss [94, 95].

5.7.2 Price discovery

One substantial benefit of an electronic market is that it produces up-to-date price information that can be shared with market participants. In our design, such information is particularly valuable to sellers, since they can benefit by reasoning about likely market prices when deciding how to bid. (In contrast, because our market design offers dominant strategies to many buyers, they have much less need to pay attention to historical price information.) To meet this need, our implemented auction system provides an interface through which buyers and sellers can learn the previous day's prices for given commodities.

5.7.3 Robustness to shill bidding

A shill bidder is an insincere bidder (or, in some cases, a sincere bidder bidding under a second identity) who bids in order to extract more surplus from a sincere bidder. Our market design is robust against shill bidders, as follows. Because both sides of the market make sealed-bid offers that are revealed only when the market clears, neither side has the opportunity to place shill bids in response to information learned about a counter-party's bid. Placing extra bids under a false identity cannot benefit a buyer, because he already obtains all of the surplus in any trade, with the seller taking the amount of his own bid. Thus, shill bidding will only drive up the price a buyer pays. A shill bid can indeed yield a higher price for a seller; however, the effect is identical to placing a higher bid, making shill bidding useless.

5.8 Conclusions

Motivated by evidence that previous approaches to mobile markets in developing countries are ineffective, and that serious inefficiencies exist in traditional trading methods in countries such as Uganda, we have designed and implemented a sealed-bid, double-auction-based mechanism that is more compatible with the needs of buyers and sellers. In particular, it is parsimonious in terms of communication and offers a dominant strategy of truthful bidding to buyers.

6 Evaluation of an incentive compatible auction system for agricultural trade

This chapter presents a discussion of the design decisions we under took for the auction system and reputation mechanism to maintain an incentive compatible market for agricultural produce. The sections in the chapter showcase the initially proposed auction interaction protocols and assumptions for the market environment. The results and evaluation section presents the outcomes for the field trials that we conducted through field visits and radio advertising. In section 6.2 we present design considerations that we made in coming up with a robust reputation system for the auction market. Section 6.4 presents results and evaluation of our study. Section 6.5 presents a conclusion to the study.

6.1 Introduction

Our work with Kudu started with a major aim of building an auction market for agricultural produce that could be operated using the readily available feature-phones in developing countries. At the start of this project we had several assumptions about the Ugandan market environment in which the system was to be piloted. These assumptions ranged from the use of village level brokers to verify produce submitted to the market and distribution of market information using primary and secondary school contacts to popularize the system in rural communities. All these assumptions among others formed a basis for initial implementation decisions for the auction mechanism and subsequent implementation iterations. This chapter presents a chronological journey of our research work that led to the final design of the auction market for agricultural produce presented in chapter 5.

6.2 Initially proposed reputation system design

This section presents design techniques that we considered in our design of a reputation system to facilitate mobile-phone based trading following a market design

that was presented in section 5.4. The reputation system design presented here follows from the reputation system goals discussed in subsection 5.6.1.

This section seeks to address various questions that arise from readers that wish to know whether other design methods could have been feasible for our proposed auction mechanism.

Section 5.2 highlighted some of the challenges arising from the presence of malicious entities and uncooperative activities in the market. Actions such as a trader not showing up at a farmer's location after committing to a purchase would be likely to frustrate farmers. Farmers also lying about the quality of their produce would hurt traders' profit margins and trader expectations. A reputation system design is hereby proposed to reward good behavior with an indication of high reputation scores and lower reputation values for uncooperative and malicious participants.

The reputation attributes considered in this setting presume an organization of traders, brokers and farmers into cooperative groups for purposes of accountability. This arrangement would be considered useful for trade environments in developing countries where people are loosely connected to permanent residential addresses. In cases of redress, these groups would provide a strong starting point for carrying out investigations and tracing sought after individuals. It is assumed that the people forming any group are known to each other. Such associations are expected to encourage rational behavior and truthfulness so as not to fail their group members.

6.2.1 Considerations for reputation scores

The initial design requirements for the reputation system was to have the registration process requiring farmers, brokers and traders to be organized into groups of at least three individuals. We expect participants to rate each other based on a scale of $1-5$, representing $Poor$, $Fair$, $Good$, *Very Good*, and $Excellent$ experiences. We use this feedback to generate scores on a scale of $(0, 1)$ to represent the aggregation using a better distribution [96]. Since the *beta distribution* is a continuous probability distribution defined over the interval $(0, 1)$, we map these score as follows: ($1 \rightarrow 0.2$, $2 \rightarrow 0.4$, $3 \rightarrow 0.6$, $4 \rightarrow 0.8$, $5 \rightarrow 1.0$). Note that these are the α values. We obtain β values using $(1-\alpha)$. After obtaining the α and β scores from transactions ratings defined over a range of $1-5$, the overall reputation for any given user can be obtained using the formula:

$$reputation\_score = \alpha/(\alpha+\beta) \tag{6.1}$$

An alternative reputation scheme would involve aggregate reputation scores that are normalized to a maximum value of 100 for all individual participants and their

groups. The purpose for normalizing to 100 is to offer an easy to understand % age scale for comparison purposes. The choice of this figure takes into consideration the societal challenges of low literacy standards in developing countries. A normalizing range between 1 and 10 would be very small for representing the accumulated reputation values. A range beyond 100 would also pause comprehension challenges for traders of agricultural produce on mobile devices. A range between 1 and 1000 would for example present figures such as 743 or 879. Such values would not be reliably understood as compared with percentage scores between 0 and 100.

We also need to limit the overall number of transactions that are to be considered for computing the user and group reputation scores. If we considered the entire transaction history, then the reputation values would grow very big for well behaving participants. Such reputation scores would encourage some users to behave maliciously in some of the transactions, with the strategy that a minimal number of malicious acts would have little impact on their overall reputation score. Reputation information based on the most recent say 500 transactions would provide a meaningful representation of the user's recent behavior and would hinder possibilities of attacks that take advantage of very high reputation values. A negative rating would for example have a big impact on someone with a reputation score from 50 transactions than one with for example 10000.

6.2.2 Positive ratings

Positive ratings in the market are used to promote social good. It is anticipated that when traders, brokers or farmers receive positive feedback, then they would be encouraged to reciprocate the positive acknowledgement with good behavior. A high reputation score would be an indicator of good behavior for a market participant. Thus individuals with high reputation scores are considered more trustworthy than those with low reputation scores. Consequently, the market design is such that high value business opportunities are recommended to reputable individuals. The proposed market design provides for traders and farmers filtering trade partners based on a range of reputation scores. This implies that individuals with very low reputation scores would not readily get favorable business opportunities in the market.

We propose positive rating contributions that are directly proportional to the level of trust that the market has in a given transaction. Market participants would earn positive reputation ratings that are weighted against $\epsilon \in (0 \ldots 1)$. If a transaction involves only trusted entities, then positive rating of $+1$ is assigned to all those involved in the transaction. Since it is not possible that all parties participating in a transaction would have perfect reputation scores, the weighted positive rating would always be less than 1 in majority of the transactions.

It is worth noting that the positive rating of $+1$ is assumed in circumstances where the parties involved do not explicitly rate each other, i.e., a trader rating the farmer and the farmer also rating the trader. It is uncommon in digital markets such as EBay to have the buyer rated. The agricultural market and the trade environment for developing countries necessitates such measures. A traders reputation is important since the nature of trade for agricultural produces provides room for the buyers or traders to act fraudulently. As noted in subsection 5.2, it is possible for traders not to deliver on their promises and thus hurt the farmer's plans. Participants in any given transaction are expected to rate each other on a scale of 1 to 10. This rating is captured as a fraction out of 10 and again weighted against the overall trust the market has in a transaction. The overall trust in a transaction $TransTrust_{Score}$ is defined by the reputation score of all those involved in the transaction and the ratings for the groups to which they belong. An individual with a high reputation score participating in a transaction with highly reputable people would earn a positive rating close to $+1$ for a successfully completed transaction.

A good reputation in the market would lead to several buyers gravitating towards a reputable seller. We additionally propose to have reduced transaction fees for reputable participants in market transactions. The value of the discounts would be computed proportionally to the accumulated reputation. Since the market design provides for buyers and sellers to filter their bids based on the reputation scores, it is highly likely that a large number of high value business opportunities would be given to individuals with good reputation values.

6.2.3 Negative ratings

Negative ratings just like the positive rating presented above, provide a scheme for discouraging bad behavior or moral-hazards. We propose a scheme in which a negative rating of -10 is weighted against the trust in the transaction ($TransTrust_{Score}$) and reduced from the defendant's overall reputation score. If the overall transaction trust is 1 then the weighted negative rating assigned to the transaction defendant would be -10.

The purpose for this big reduction is to promote truthfulness in the market while substantially reprehending bad behavior. The market design does not facilitate individuals to quickly build high reputation scores. In retrospect, it takes a few dishonest transactions for market entities to have their reputation largely reduced. In so doing, we expect the market to progressively eliminate untruthful characters since the results of their actions would be quickly reflected in the reputation scores.

Negative ratings are assigned to farmers or traders, in case either party is unhappy with the outcomes of a transaction. A trader may find that the goods promised by

the farmer are far below the anticipated quality. Such a scenario might arise from a farmer colluding with a broker to mis-represent the status of their produce. In such circumstances, the trader would raise a negative rating for the farmer and broker involved in the transaction. It is also possible for the broker to faithfully review the produce, but the farmer goes ahead to exchange what was reviewed with the poorer quality. Such acts can still be punished and the broker exonerated through the arbitration process presented at the end of this section. The brokers cannot issue negative ratings since they are passive participants in the transactions.

It is also plausible that some participants would retaliate on receiving low ratings from other participants. Since ratings are from entities that together participated in a given transaction, it would be easy to detect retaliatory ratings from the patterns of reputation scores. Furthermore, negative ratings might attract colluding participants into giving negative ratings. Such an attack would not be successful since ratings are only allowed from entities that together participated and completed a transaction.

The negative ratings cannot be assigned by the market participants. These ratings are to be assigned after an arbitration process between the parties involved in order to determine the individuals that were at fault.

6.2.4 Groups and reputation scores

The group setups are used to foster accountability from all the market participants. It is assumed that individuals that form a group are fairly known to each other. For example, these might be people residing in the same location or trading from the same market area. Each member of the group would receive a fraction of **one hundredth** of the reputation score earned by a member's transaction. The fraction contribution is computed based on the number of members in a group. Given a group j with n members, and a reputation score $RS_{i,j}$ earned by i a member of group j, the reputation earning for each group member would be $(\frac{RS_{i,j}}{100} \times \frac{1}{n})$.

The additions or deductions of reputation points occur whenever positive or negative ratings are earned by any of the group members. The purpose for additions and deductions from group members is to encourage peer pressure and a self monitoring system for the market in which peers hold each other accountable for their actions. All group members would receive message alerts for rating additions and deductions. It is anticipated that such openness for group contributions would enable group members to monitor each other and thus promote good behavior. Group contributions are likely to further present incentives for group members to maintain a small group of people that would not let them down. Additionally, smaller groups would have higher average single contributions than larger groups. However, the frequency

Stakeholders and Reputation Attributes		
Farmer	**Broker**	**Trader**
Farmer's Reputation (F_{Rep})	Broker's Reputation (B_{Rep})	Trader's Reputation (T_{Rep})
Farmer Group (FG_{Rep})	Broker Group (BG_{Rep})	Trader Group (TG_{Rep})
Successful Transaction (ST_{Score})	Successful Transaction (ST_{Score})	Successful Transaction (ST_{Score})
Failed Transaction (FT_{Score})	Failed Transaction (FT_{Score})	Failed Transaction (FT_{Score})
×	×	×

Tab. 6.1.: *Mobile trade stakeholders and reputation attributes*

of contributions would be higher for larger groups than smaller ones due to a higher probability of a group member carrying out a transaction.

Given xg_i, yg_i and zg_i respectively as group reputation scores for farmers, traders and brokers, whenever a transaction is successfully carried out, xg_i, yg_i and zg_i are incremented by one-hundredth of the *"successful transaction score"* (ST_{Score}) and otherwise reduced by one-hundredth of the *"failed transaction score"* (FT_{Score}). The *"successful transaction score"* and the *"failed transaction score"* (FT_{Score}) are weighted against the overall trust that the market has in the given transaction before being used in any additions or deductions. Table 6.1 presents a summary of attributes for the reputation scores in the trade environment.

6.2.5 Ratings for new market entrants

The earlier design considerations for the registration process was expected to be done off-line (manually) so as to eliminate possibilities of capturing fake identities (sybils) which might later on be used for self promotion. An example of such a registration attack would be a broker that registers themselves with a second profile as a farmer using different mobile-phone numbers. Such a broker would be able to submit produce with one identity as a farmer and at the same rate it highly as a broker. The off-line registration process is expected to be carried out in villages and trading centers after verifying identity cards of the individuals. This kind of scheme is currently showing success for mobile-money services in Uganda.

We propose not to have a defined reputation value for new market entrants. A new market entrant is defined as one that has not yet performed a single transaction. The visible global status of such individuals would be represented as "New entrant". New entrants would earn a reputation score after performing at least one transaction. The new entrant does not also receive reputation scores from the group before completing a transaction of their own.

6.2.6 Normalizing ratings

All ratings that are received from end-user input are supposed to be normalized so that we prevent errors and malicious collectives from distorting reputation scores. It is possible for example in the ratings of produce for the brokers to erroneously rate the produce with a rating that is above 10. Additionally, malicious elements in the market might also try awarding their accomplices positive ratings outside the allowed range. Input validation for SMS submissions would be used to eliminate possibilities of malicious and erroneous entries. A messaging alert system with a limit for the number of erroneous messages permitted would be used to remind users about incorrect submissions.

6.2.7 Considerations for user registration

The registration process is used to capture information concerning market participants. This information includes group composition details, participants' locations and their product preferences. During the registration process, we expect farmers, brokers and traders to indicate their products of interest. This specificity is important so that the market messaging system does not simply send all registered users in a given location requests for items in which they have no interest.

The registration process for the market participants follows the process listed below:

1. Each category of market participants (farmers, brokers and traders) identify at least three people known to them as possible group members. Each member is supposed to belong to a single category of market actors. It is not acceptable for someone to register in a farmer group and at the same time register as a broker or trader. The group sizes are also restricted to a maximum of 10. The purpose for this is to encourage group formation amongst people known to each other. A large group would most like have people little known to each other. The other issues related to contributions of group reputation scores were also presented in subsection 6.2.

2. The members of the created group present their identity cards and mobile numbers at the registration center. The purpose for physical examination of identity cards is to prevent users from creating or registering sybil profiles.

3. Each participant in the market is also assigned a secret or password that would be used to update their profiles via the mobile phones.

4. In additional to personal details information, the registration process would be required to capture the details listed below concerning the farmer and their group.

    - Group Identifier : This is a unique identifier for the group to which the group members belong.

    - Group Secret : The group secret would be used in a challenge response protocol for updating group membership lists.

5. Location Identifier : The location identifier is used by the market system to route alert messages to individuals nearest to their trade partners. Traders, Brokers and Farmers can also filter their requests based on the distance from the farmer, broker or trader. Brokers and traders might for example not be able to pursue business opportunities beyond a given distance measure. These distance preferences would be captured using the location identifiers.

6. Product Preferences: A farmer would for example register products which they would be able to supply to the market so that they do not receive message alerts for products that they cannot provide. Traders not interested in beans for example should be able to express this preference too, such that they do not receive alert messages for beans. Furthermore, brokers should also express the products that they would be able to evaluate. The system design and implementation should also provide means of updating this list of preferences.

Interactions and message exchanges between the farmer, broker, trader and market are presented as an interaction protocol in the subsection 6.2 below. The interaction protocol shows various ways in which the reputation information impacts trade decisions in the mobile-based market environment. This protocol assumes reputation information which is represented as a numeric score. Such a score could be awarded on a scale of 1 to 10; whereby 1 represents unacceptable behavior and 10 for the most trusted or acceptable behavior. The range of 1 to 10 comes naturally to the people in the great lakes region of East Africa. It so happens that several ancient stories in the Ugandan region have this range (1 to 10) in their comparison schemes. Additionally, the range of 1 to 10 also provides a good scope of evaluation for produce quality. The continuous range of ratings between 0 and 10 is fairly easy to translate into a quality rating for produce.

6.3 Evaluation of our initially proposed market designs

The final design that was presented in section 5.4 proved to be robust during the pilot phase. The market design that was initially proposed in section 5.3 had several shortcomings which are discussed in the listing below;

- Subjecting market participants to a group setting was introducing bottlenecks in the registration phase and user adoption rate. Users complained about the time it took for them to find users that were as enthusiastic to join the system. This difficulty was clearly understandable to us since the system was new and most people have been accustomed to word of mouth marketing of their produce.

- Group schemes for reputation had a huge messaging overhead for system operators. The number of messages exchanged between the system and farmers or traders increased by a magnitude directly proportional to the number of group members. In the absence of group settings, a single message notification was sufficient.

- The proposed reputation mechanisms in section 6.2 were still susceptible to extortion attacks. Users in the market would have a possibility of threatening their counterpart to give them a high rating in exchange for some favors. On the others hand, the blacklist scheme proposed in section 5.6 presents the right incentives for users to rate each other fairly. If a buyer has received a good deal from a seller, they would not want to blacklist such a seller since the buyer would wish to meet such a seller again.

6.4 Results and evaluation of the final system design

In order to evaluate our market design approach and environmental assumptions, we conducted field trials in separate phases. The first phase took place during September 2012 aimed at testing basic usability assumptions,the second evaluation phase was started in January 2013 to August 2013. The most recent pilot executed from January 2016 to April 2016 in partnership with the Innovations for Poverty Action (IPA)(http://www.poverty-action.org/).

The system was made accessible to users throughout Uganda via a toll-free SMS short code (8228). We communicated information about using the system to sellers with a series of meetings in districts in farming-intensive regions of central Uganda, as well as via radio broadcasts. Buyers were also recruited using radio broadcasts in Kampala, and visits to wholesale markets to hand out flyers explaining system

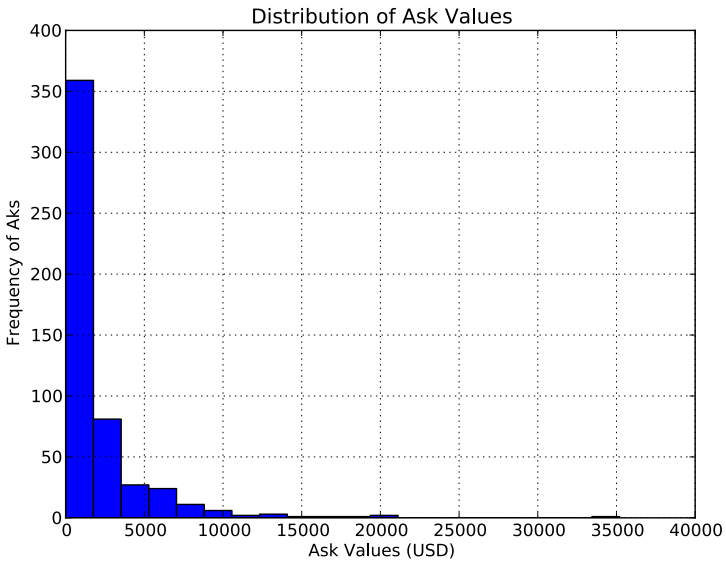


Fig. 6.1.: *Distribution of asks for all products in the market (2013 trial).*

Month	Total Asks	Total Bids
Jan	56	23
Feb	130	61
Mar	210	173
Apr	378	268
May	469	284
Jun	500	285

Tab. 6.2.: *Cumulative numbers of asks and bids received in the period January–June 2013.*

functionalities to potential users. We began with four commonly traded staple crops (coffee, maize, beans and peanuts) and added new produce categories to the system through user demand. The market currently has 70 produce categories.

6.4.1 Quantitative results

The auction market has been active since January 2013 and has been available mostly in the central and south-western areas of Uganda. A total of 1024 traders and farmers were registered between January and July, 2013. The total count of bids and asks was 316 and 566 respectively. Not all registered users submitted bids and asks: 219 users only used the system to ask for commodity prices. The total value of asks from sellers was USD $1,700,000, and the total value of bids from buyers was USD $960,000. Table 6.2 shows the cumulative numbers of bids and asks each month. Bids and asks tended to be large quantities from wholesale traders; for instance the largest bid received was for 120,000 Kg of maize (we verified the

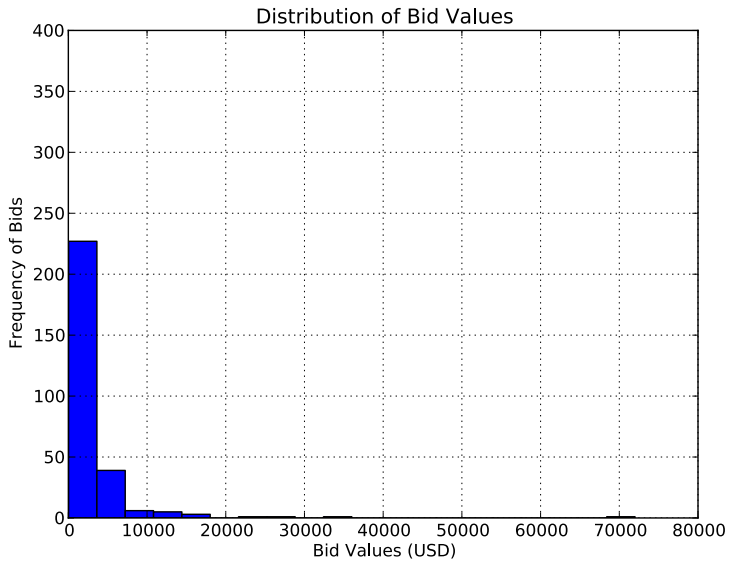


Fig. 6.2.: *Distribution of bids for all products in the market (2013 trial).*

Produce type	Total ask quantity
Peanuts	512,375 Kg
Maize	1,711,935 Kg
Beans mixed	114,900 Kg
Coffee (Robusta)	36,800 Kg
Sweet Potatoes	2,221 Sacks

Tab. 6.3.: Quantities of the five categories of produce with the highest aggregate ask value (2013).

details with the buyer and found the bid to be genuine). We received 53 bids and 94 asks for quantities exceeding 10,000 Kg. Figures 6.1 and 6.2 show the distribution of bids and ask values for all products in the market.

Table 6.4 shows the total quantities of bids on the five produce categories with the highest total bid values, and Table 6.3 shows the total quantities of asks on the five produce categories with the highest total ask values.

We observed that market activity was highly dependent on the frequency of radio adverts. The increase in the number of bids and asks was significantly higher in months that had a higher frequency of adverts than those months with fewer adverts. We attribute the low growth in May and June to this factor.

We sampled 30 unique mobile numbers from a list of 1,748 matches that occurred in the market between the first of January and the first of July, 2013. We identified 4 users that registered successful transactions that led to exchange of money,

Produce type	Total bid quantity
Maize	917,300 Kg
Sesame	110,000 Kg
Beans mixed	179,050 Kg
Soya	40,000 Kg
Peanuts	35,050 Kg

Tab. 6.4.: *Quantities of the five categories of produce with the highest aggregate bid value (2013).*

Commodity	No. Asks	No. Bids
Maize	235	78
Simsim (Sesame)	1	3
Beans mixed	24	33
Soya	14	6
Peanuts	15	14
Coffee (Robusta)	17	5
Potatoes	40	20

Tab. 6.5.: *Distributions of bids and asks for the top 7 crops (2013).*

representing a 13.3% success rate, albeit in a small sample. We also received calls from 28 buyers and sellers who offered (unsolicited) feedback by calling the helpline number, which helped us to confirm that real trade was occurring as a result of the matches proposed by the system.

The market registered a total of 74 agricultural commodities that were all populated based on farmer and trader market demands to sell and buy these particular products. The top 7 crops for both Bids and Asks submitted to the market during pilot period were; Maize, Simsim, Beans mixed, Soya, Groundnuts, Coffee and Potatoes. The distribution of asks and bids among the popular commodities was as shown in the table 6.5;

6.4.2 Evaluation of user perceptions and experiences

The market system registered its first 500 users in February 2013, a month and half after starting the pilot (see Figure 6.3). We were encouraged by such quick adoption, considering that users had no previous experience with a similar system.

Notwithstanding the encouraging adoption numbers, users have raised several issues regarding the usability of an SMS-based interface. While we attempted training sessions and radio announcements explaining message formats such as 'BUY

Commodity	Matches
Maize	444
Simsim (Sesame)	1
Beans mixed	83
Soya	17
Peanuts	22
Coffee (Robusta)	19
Potatoes	117

Tab. 6.6.: *Distribution of matches between the top 7 commodities (2013).*

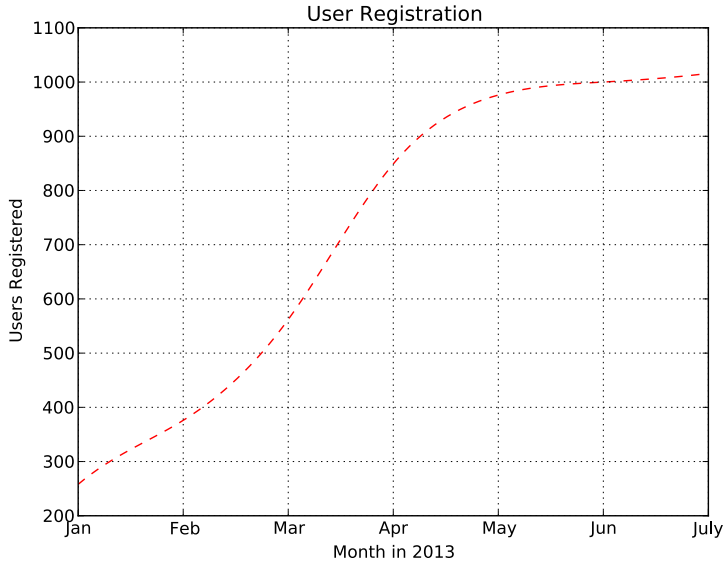


Fig. 6.3.: *User registration in the market (2013).*

[PRODUCE] [QUANTITY] [UNIT PRICE]', almost all the messages we received did not follow this format well enough that they could be parsed automatically. The most common issues were variations in spelling, ambiguous figures, or messages written in free text. In practice, whenever a malformed message is submitted to the market, we decipher meaning from the message if possible and then resubmit it on the users' behalf. In circumstances where we cannot derive the meaning from the message, we typically call back the sender to confirm their intentions. We note that this would present difficulties if we faced very large volumes of senders, though note also that labor costs are low enough in Uganda that considerable manual intervention remains feasible. We plan to mitigate this problem with a USSD interface or an interactive voice response system. Concerning the SMS interface, we also found user feedback to be more positive in the second phase of trials when the SMS system was translated into local languages, even for those who had no problem communicating in English.

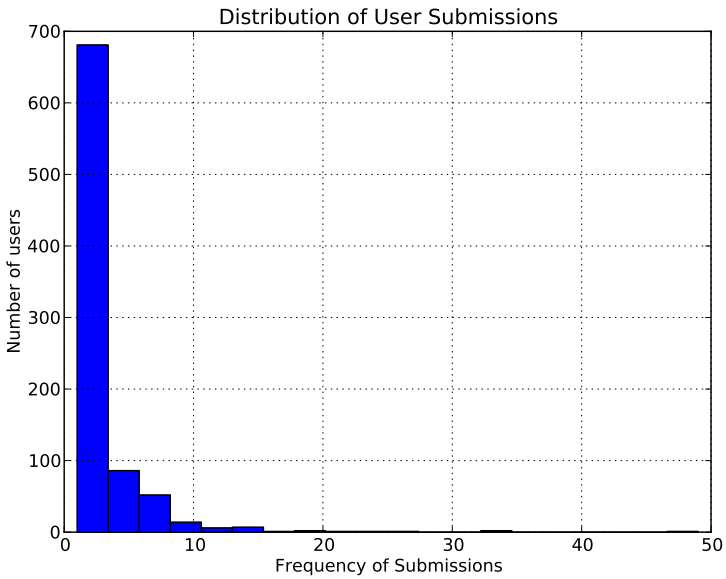


Fig. 6.4.: *Distribution of user submissions to the market (2013).*

The mobile auction system was more quickly adopted by sellers than by buyers. This seems to represent the fact that buyers have a stronger position in the current market, and therefore less to gain by adopting a new system. However, we observed particular interest from large-scale buyers, who face challenges in sourcing bulk quantities of produce for export or factory processing.

The addition of new product categories on the market was demand driven. Most of the species added were not anticipated by us at the outset of the field trials. Some new products were added to the market on request and we saw immediate popularity among both buyers and sellers. For example, we did not expect to sell animal hides; a hides-and-skins buyer contacted us with a desire to find sellers. Once the item was listed on the market and an announcement made on radio, 10 sellers were enrolled and 10 matches happened as a result. Other unexpected produce categories in which we saw market activity were eucalyptus poles, pineapple suckers, ginger, and soya, the latter becoming a significant commodity as shown in Table 6.4.

We have seen several farmers act as aggregators for produce in their areas in order to complete a large volume sale. We also find that brokers are able to become users in our system, performing an important role of produce aggregation. The majority of farmers do not grow produce in the large quantities that are sought after by traders, making such aggregation a powerful approach to produce marketing.

In general the speed at which users grasped the double auction concept has impressed us; we find this to be compelling evidence that our proposed system is more effective

than traditional methods of agricultural trade. The market system had several repeat users as shown in the distribution of user submissions in Figure 6.4.

Commodity	Matches	Estimated Deals (13.5%)
Maize	444	57
Simsim (Sesame)	1	1
Beans mixed	83	11
Soya	17	2
Peanuts	22	3
Coffee (Robusta)	19	2
Potatoes	177	23

Tab. 6.7.: *Comparison between matches and actual deals that were completed for the top 7 commodities (2013 trial).*

6.4.3 Analysis of matches between buyers and sellers

This subsection analyzes the distribution and results of matches between buyers and sellers that took place using the automated matching algorithm presented in section 5.4.

We allowed for a maximum of 3 matches for each ask during the pilot to increase the probability for a farmer to find a highly interested for a transaction to exchange cash. This was particularly useful since the system was not handling payments that would enable us to actually tell whether a transaction had gone through. The only means of knowing whether a transaction had gone through was when sellers and buyers volunteered call backs through messages of gratitude or when we called them back during the data sampling phase.

Another approach we think could help us in determining success is to integrate the platform with mobile-money such that buyers and sellers register escrow accounts that would be used to temporarily hold funds on behalf of the buyers that would only be released to sellers once the buyer has accepted the dominant match on the Pareto frontier as defined in section 5.4.

Table 6.6 presents a distribution of matches between top 7 popular commodities.

We observed from the dataset that some popular products such as maize registered scenarios of repeat bidders or frequent buyers that had their bids recycled particularly because they want to buy the same produce without resubmitting bids. The design of the platform allowed the interface administrator to re-register such bids on behalf of the buyers.

Table 6.7 presents a comparison between matches and estimate matches that resulted into actual exchange of cash between farmers and traders.

6.4.4 Robustness of user reputation mechanism

Trust can be difficult to achieve in electronic markets: when market participants are relatively anonymous, bad behavior (failure to honor an agreement; attempting to trade in produce which is adulterated or otherwise below a reasonable standard) can go unpunished, and traders therefore become cautious. To mitigate this problem, it is necessary to institute some kind of reputation system in the market, to give traders information about the reliability of the buyers or sellers with whom they are matched [97, 98, 99, 100, 101].

The most common form of reputation system asks traders to rate their counter-party after a trade has occurred. (For example, such a system is prominently used by eBay.) However, we did not consider such a system to be appropriate in our setting. For example, we were concerned that a buyer could extort a positive rating from a seller at the moment of sale. We thus sought an alternate reputation system. Our goal was to construct a system that would be resistant to the following forms of attack:

(self-promotion) users can dishonestly increase their own ratings;

(slander) users can insincerely decrease the ratings of others;

(whitewashing) users can discard an account with a bad rating and obtain better reputation by starting anew;

(sybil) users can create false profiles and use them to give themselves a positive rating.

We elected to use a reputation system with two components. First, we track positive ratings implicitly, via trades that are accepted by both parties. Second, we track negative ratings explicitly, by giving participants the opportunity to blacklist the mobile numbers of counter-parties with whom they have previously been matched, and with whom they want to be guaranteed never again to be matched.

This system resists the four forms of attack previously discussed as follows.

(self-promotion) Positive ratings in the market are captured from successful completed transactions as opposed to user-submitted ratings. In our scheme self-promotion is not possible since all participants are considered to have behaved positively towards each other unless they are blacklisted.

(slander) Slander is costly, as false blacklisting denies a trader future access to a counter-party. This strongly reduces the possibility of participants threatening each other with low rating scores. Furthermore, since blacklisting is only allowed between parties that transacted, bulk slander is impossible.

(whitewashing) The attachment of mobile numbers to the registration process imposes a cost to whitewashing: the registered mobile numbers are the ones that the market system uses for communication purposes.

(sybil) The success of sybil attacks depends on the cost required for creating a new profile [99, 102]. In our system, the centralized user registration process increases the cost of sybil attacks: each sybil profile needs a distinct, active phone number to participate in the market.

Results of the blacklisting reputation mechanism

This subsection discusses results of the reputation scores that we experienced during the pilot.

Farmers that blacklisted traders (blacklisted traders) were: 1
Traders that blacklisted farmers (blacklisted farmers) were: 4

All the farmers that were blacklisted resulted from the sale of a variety of cassava that the buyers said had a bitter taste. A farmer never wanted to be matched again with a trader that promised to buyer her produce and requested her to make it ready but never turned up.

We received a total of 5 blacklists. Blacklisting of a buyer or seller is performed on the basis that there was match (— transaction history —) between these two entities. If a given user mobile number has not traded before with another, the blocking request will be notified as not permitted.

The reputation scores are also used in determining the Pareto optimal matches. A user that has been blacklisted will not have an ask that dominates an ask from a seller that has not been blacklisted. Sellers or buyers that had been blacklisted would be rated low on the matching algorithm.

6.4.5 Results from 2016 trials

During the first agricultural season of 2016 (January to March 2016) we carried out a randomized control trial (RCT) in partnership with IPA (http://www.poverty-action.org/) in 20 districts of Uganda. The control and treatment dis-

Produce type	Total ask quantity (Kgs)
Maize	10,985,131
Beans (Nambale)	1,654,925
Beans (Yellow)	870,100
Rice (Kayiso)	97,000
Millet (Bulo)	25,000

Tab. 6.8.: Quantities of the five categories of produce with the highest aggregate ask value (Jan to March 2016 season).

Produce type	Total ask quantity (Kgs)
Maize	14,621,346
Beans (Nambale)	688,000
Beans (Yellow)	102,800
Simsim (Ntungo)	430,300
Rice (Kayiso)	55,000

Tab. 6.9.: *Quantities of the five categories of produce with the highest aggregate bid value (Jan to March 2016 season).*

tricts were even distributed across the country from the Central, Southern, Eastern, Western and Northern areas of Uganda. The field trials were carried out during this period through field visits by a group of field agents that taught sellers and buyers of agricultural produce on how to use the platform.

We obtained a total of 2900 new users registered on the platform and 383,000 kilograms of grain traded through the platform. The produce that was traded on the platform amounted to $135,831 USD during the first agricultural season of January to March 2016.

Presented in the tables 6.12, 6.9, 6.10 and 6.8 is a qualitative listing of buyer and seller activities during the January to March 2016 period.

A second market update happened in the agricultural season of June to September of 2016. During this period, we used radio broadcasts to advertise to listeners in 22 districts of central Uganda. The cumulative user registration graph in figure 6.5 shows a sharp increase in the number of user registration between May and September 2016.

Table 6.11 presents the total number of Asks and Bids that were submitted to the market for the two (January-March and June-September) 2016 seasons.

Commodity	No. Bids	No. Asks
Maize	783	1131
Beans (Nambale)	96	245
Beans (Yellow)	16	70
Rice (Mukyele-Kayiso)	3	9
Cooking Bananas	2	7

Tab. 6.10.: *Distributions of bids and asks for the top 5 crops (Jan to March 2016 seasons).*

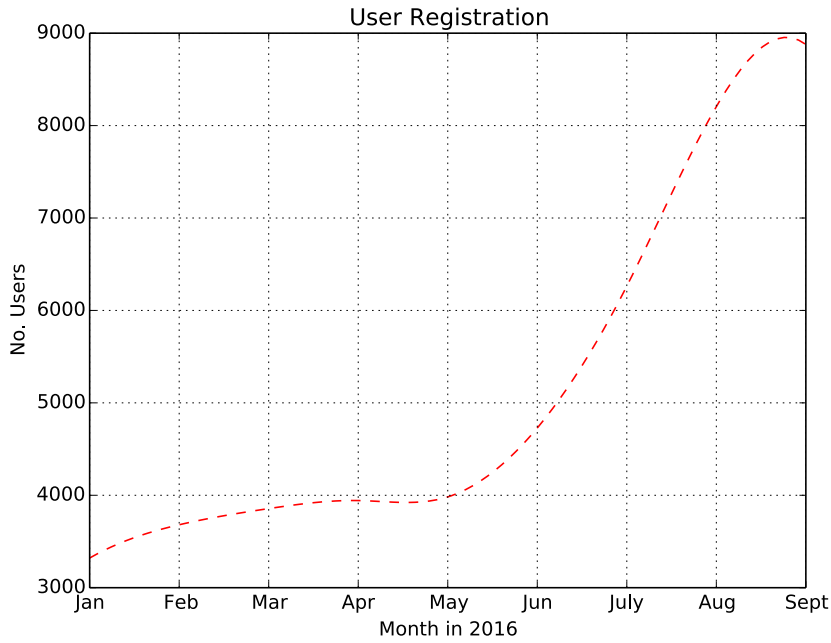


Fig. 6.5.: *Cumulative user registration in the market (2016).*

Tables 6.12 and 6.13 represent deals that traded on the platform the January and June seasons respectively. We see from the transactions that were concluded in the two seasons of 2016 that the market adoption was good and an enthusiastic response based on buyer bids and seller asks in table 6.11.

We also observe that the rate at which bids and asks are converted into transactions or deals is still low. We for-example registered asks worth USD 29.7 million but had a total of USD 445,000 in transactions. A close analysis of the data indicates that a large percentage of Ask prices were above the Bid prices. This phenomenon is attributed to user expectations for a new market system. Buyers typically expect a new market platform to provide them with access to commodities with lower prices than the existing old-channels. Consequently, buyers submit low bid prices with anticipation of finding good matches with sellers. Sellers on the other-hand also have anticipation for the new market system to help them find new-buyers with

Commodity	Bids Value (USD)	Asks Value (USD)	No. Bids	No. Asks
Maize	52,194,368	22,135,305	4,196	12,588
Beans	9,167,706	4,269,704	1,315	3,945
Soya	4,265,974	2,339,999	557	1,671
Simsim	1,645,439	210,642	108	324
Groundnuts	1,004,212	241,845	187	561
Millet	227,727	28,315	103	309
Rice	192,700	439,597	151	453
Sorghum	71,845	63,443	59	177
Totals	68,769,972	29,728,851	20,028	6,676

Tab. 6.11.: Comparison for count of Bids and Asks with Dollar-value for the top 8 commodities (January to September 2016). We observe from the table that the dollar value of Bids is much higher than that of Asks despite Asks having a higher rate of requests than Bids.

Commodity	Number of trades	Quantities (Kgs)	Total trades (USD)
Maize	32	249,000	56,590
Rice (Kayiso)	5	64,000	38,787
Beans Nambale	6	60,000	36,363
Beans Yellow	1	10,000	6,666
Total			138,406

Tab. 6.12.: *Top 4 deals that were completed on the market platform (Jan to March 2016 season).*

better buying prices than their existing channels. This situation typically creates few matches that are feasible between buyers and sellers despite having a large number of bids and asks.

6.5 Conclusions

Based on the quantitative results, our auction mechanism design received enthusiastic adoption among buyer and sellers of agricultural produce. Field trials with a web- and SMS-based implementation have shown enthusiastic adoption and significant trading activity, providing strong evidence that our market platform meets local needs.

Previous approaches to solve the information asymmetry and market efficiency problem have largely tried to implement price advisory services, which we argue have not been effective. Price advisory systems struggle with data accuracy and relevance, given market participants' strategic incentives to misreport prices. Other

Commodity	Total trades (USD)
Maize	205,143
Beans	72,364
Groundnuts	4,397
Rice	14,470
Soya	10,075
Total	306,449

Tab. 6.13.: Transactions (Deals) that were completed in the second agricultural season (June to September 2016).

attempts to implement market services have most been classifieds or single auction systems. Classified listings and single auction mechanisms require a significant amount of information to communicate or represent an item electronically. This technically requires an internet-enabled phones (which are not widely available) in order to represent all the required information. These systems fail to capitalize on the fact that agricultural goods are commodities.

Our proposed market design and implementation is a mobile-phone-based market that offers a better alternative. Unlike all other systems, our proposed market mechanism uses a sealed-bid double auction to achieve an effective and practical electronic market for agricultural commodities. Notably, it operates efficiently over SMS–with trades requiring only a small number of 160 character messages in one of several local languages—thereby making it accessible to the majority of farmers who lack internet-enabled phones. The system offers bidders incentives to place sincere bids, tracks their reputations, and accommodates geographical constraints. It uses bids to propose a match that both parties are free to decline; if both accept, the system proposes a price, but traders are free to negotiate based on the quality of produce being traded.

7 Epilogue

In this thesis, we have studied the consumer buying behavior in Ugandan agricultural markets, with a goal of providing a new and effective market-mechanism that alleviates existing problems of information asymmetry and trust in an open distributed environment. This chapter summarizes our work and provides a highlight of our contribution in the context of the consumer buying behavior.

7.1 Thesis overview

This thesis has presented a general outlook of agricultural trade in Uganda and presented a general representation of agricultural markets in developing countries using Uganda as a case study. The research work for agricultural markets in developing countries was approached with the aim of improving market efficiency for trade in agricultural produce. This objective was motivated by an analysis of historical agricultural market data to determine the presence and extent of temporal and spatial arbitrage opportunities. As presented in chapter 2, the analysis results indicated a strong presence of spatial and temporal arbitrage opportunities.

The large presence of such high levels of market inefficiency is largely attributed to poor forms of market information exchange. Market information in developing countries such as Uganda is performed using word-of-mouth techniques and through a wide presence of mobile cellular networks. These techniques unfortunately do not scale beyond the already established circles of interaction between friends, family and acquaintances.

This thesis builds on consumer buying behavior models to develop a solution which supports automated negotiations and secure interactions in various stages of the auction mechanism with participants. We have presented a collection of techniques for agent-systems which are used to model and design automated interactions between buyers and sellers. We have also presented digital security techniques for providing integrity of messages exchanged and presented a comprehensive solution for enabling privacy and confidentiality in an open distributed environment.

Previous attempts to create electronic markets have yielded systems which are not compatible with buyer and seller needs in the Uganda market systems. Despite some

of these efforts having been supported by large organizations, they did not create the right combination of technology and market interaction configuration.

This thesis has leveraged on agent-modeling techniques to design an agent-mediated system for agricultural trade in developing countries such as Uganda. The design and implementation are secure in terms of privacy, confidentiality and also incentive compatible to requirements of farmers and traders.

7.2 Reflection on the research problem, objectives and questions

This research work started with a goal of investigating techniques that would improve efficiency in electronic trade using enhanced models of automation and robust security frameworks in open-distributed environments. Agricultural markets in Uganda presented unique opportunities and challenges for the study. The failure rate for electronic-commerce systems in Uganda consistently been very high over the past 10 years. Nonetheless, the rate at which attempts to create stable electronic system was made was also very high. Google was present in the East-African region with Google Trader and the Grameen foundation also had numerous initiatives. All these efforts were however falling-short of delivering a robust electronic system not-only for agricultural trade but also for other commodities trading in Uganda. Based on these experiences, it seems as if electronic-trade in developing countries such as Uganda needed an approach that was different from those established in the developed world.

These experiences and observations led us to setting a main objective of *contributing towards techniques necessary for developing secure and incentive compatible electronic-markets in developing countries*.

In order to achieve this main objective, we set out to pursue the specific objectives presented below;

7.2.1 Reflection on research objectives

i. The first specific objective was to design an incentive compatible auction market for mobile-based agricultural trade in developing countries such as Uganda.

   Having observed that several electronic-commerce systems had failed in Uganda and more-so in agricultural trade, we realized that it was very impor-

tant for the electronic-system design to not-only provide means of information exchange, but to also be incentive compatible with the participants. We need to guarantee ourselves that we were designing and creating an electronic system that would encourage farmers, brokers and traders to participate.

Agricultural markets in developing countries are largely dominated by brokers and traders who benefit from the elevated levels of market inefficiency. Any new system that is aimed at reducing their gains from the inefficiencies is likely to face an indifferent adoption. Achieving an incentive compatible systems is one of the most important attributes for a solution to market inefficiencies in agricultural trade and generally other forms of electronic-trade systems.

This specific objective is achieved in chapters 2 and 5.

ii. The second specific objective was to develop extended threat models for agent-mediated applications in an open-distributed environment.

An agent-mediated model was chosen as the approach for achieving automation in electronic-market interactions between participants. This specific objective aimed at presenting a detailed view of digital threats that are likely to be faced by a system which is implemented based on an agent-mediated model. The overall objective of this research was set-out to be practical — this meant that the deployment of the application would have to be visible to threats in an open distributed environment. In order to develop countermeasures to threats in an open-distributed environment, we need to understand them very well in the first-place and model them to the anticipation of our market design.

This specific objective is achieved in chapter 3, section 3.2.

iii. The third specific objective was to design and implement an agent-mediated auction market for autonomic trading based in an open distributed environment.

This objective was used to set the stage for achieving a practical system which farmers and traders would use to perform agricultural trade following a robust design. We also set out a goal to eliminate manual methods of market matching that were part of most failed system that had previously been launched in Uganda.

This specific objective is achieved chapter 5.

iv. The fourth and last specific objective was to test and validate the designed and implemented applications based on the defined incentive compatibility and security requirements.

In order to validate our design and implementation, we aimed with this objective to methodologically test various components of our system implementation. We wanted to guarantee security requirements and also ensure that we can test them in the open operational environment.

This specific objective is achieved in chapter 6

7.2.2 Reflection on research questions

i. What is the extent of agricultural markets inefficiency in Uganda? What factors are leading to agricultural market inefficiency in developing countries found in Sub-Saharan Africa?

This research question was posed to guide our research efforts for designing and implementing an electronic system that would be acceptable to both traders and farmers. We needed to obtain empirical evidence on inefficiencies for agricultural in Uganda. We analyzed data from FEWSNET and presented results of agricultural markets inefficiencies in section 2.4. As described in section 2.2 we visited markets in urban areas and rural areas for a period of more than one year to study causes of inefficiencies in agricultural markets and to gain a detailed understand factors leading to this problem. Results for these market evaluations are presented in chapter 2 and as such the questions answered.

ii. How can we design market mechanisms that are incentive compatible for trader, farmer and broker agents to participate in and adopt?

Having observed inefficiencies in agricultural markets from our evaluation of historical market data, it became evident that existing methods of trade were not appropriated for agricultural and commodity markets growth. It was however crucial for us to understand in detail why these inefficient methods had been practiced for centuries without pursuing alternatives as the rest of the developed world had done. We needed to understand in great detail the kind of incentives that we would have to introduce in our market designs in order to get brokers and traders who have traditionally benefited from the inefficient market configuration to participate in the new.

The objective of this question was to help us obtain parameters which would be included into the market mechanism design to create incentives for farmers, brokers and traders to participate. Our market system adoption was highly dependent on us obtaining the correct combination of attributes for stakeholders participation. This question was sufficiently answered in chapter 5 section 5.7. The high levels of enthusiasm in adoption of the market systems by farmers and traders is also a strong indicator that we sufficiently answered this question as presented in chapter 6, section 6.4.

iii. How do security threats against agent-mediated applications evolve in adversarial situations found in open distributed environments?

The objective of this question was to help us in identifying security challenges and threats in an environment for agent-mediated applications that have to interact with diverse participants. The objective of this research question was to help us derive a threat model for an open-distributed environment for the planned system designs. This question was answered sufficiently in sections 3.2,A.5 and the appendix A which clearly demonstrate the differences and similarities in threat models given deployment of application models in varied agent-mediated platforms. The thesis demonstrates the threat models using a book-trading application implemented with an automated negotiation framework A.

iv. Privacy, confidentiality and integrity are key requirements for electronic trading. How can public-key cryptography be used to guarantee privacy, confidentiality and integrity for publishers and subscribers in a multi-agent environment?

The objective of this question was to guide our efforts in pursuing privacy, confidentiality and integrity requirements for the prototype application that we envisaged to improve agricultural markets efficiency. We needed to think upfront about the challenges of privacy and data integrity in an open distributed environment. The environment for the anticipated application was modeled in section 4.1 using a publish-subscribe environment. This models imitates publishers as seller in agricultural markets and traders as subscribers. The results of our study and analysis in sections 4.4 show that our solution for privacy and confidentiality in open publish-subscribe environments strongly answers the this research question.

v. Understanding of shilling in both reputation mechanisms and auction markets is critical for autonomic electronic-commerce environments. Which techniques can be used to prevent shilling attacks in auction markets and reputation mechanisms?

Electronic markets that don't have the correct techniques to protect against shilling attacks would typically suffer from adverse-selection problems — in which bidders would always bid very low prices anticipating poor matches and buyers asking very high due to anticipation of troublesome buyers. We spent a significant research effort in finding the right ingredients for reputation mechanisms which would offer the correct incentives for good behavior but also prevent bad-acts from going unpunished. We present in the appendix 5.3.2 a detailed evaluation of some of the choices we first made. These choices appear robust and many readers would question our final design if they have not evaluated the choices that we discarded. Our final design which presents a blacklisting technique for bad-behavior is presented in section 5.6. The results of pilots studies and feedback from participants are a good indicator that we sufficiently answered this question.

7.3 Research results and contributions

In order to achieve the objectives listed in section 1.4 above, a number of contributions were made to the state-of-the-art techniques for automation and security in the consumer buying behavior model.

- Our research work in Ssekibuule *et al.* [103] presents our contribution to the development of secure negotiation frameworks in agent mediated electronic commerce systems. Our contribution focuses on the configuration requirements for a secure model of negotiation in an open distributed environment that has to protect against self-interest actors. This research work also helps developers of secure negotiation frameworks to better understand the threat environment in a holistic framework of agent interaction.

- In Ssekibuule *et al.* [104] we contribute to the design of electronic markets in environments with self-interest agents and provide an example implementation that is robust against strategic liars. Our research work in this area provides a contribution towards design requirements for applications in resource constrained environments such as those found in developing countries where people mostly use feature-phones that are not Internet connected. This research work makes a contribution more particularly to the design of robust auction mechanisms for agricultural trade in developing countries. The implemented prototype demonstrates our contribution towards application designs with a novel double-auction mechanism that offers incentives for truthful behavior in an environment with self-interest agents.

- Our research work in Ssekibuule *et al.* [105] makes a contribution towards benchmarking techniques for protecting software agents against malicious platforms. This research work presents an evaluation of state-of-the-art techniques for protecting software agents and qualified limitations for these techniques. This evaluation sets a landscape within which we developed security evaluations for an agent mediated application [106].

- In Ssekibuule *et al.* [106] we make a contribution towards the practical development of agent-mediated applications by implementing a booktrading application using two agent platforms. This research work show cases design and implementation requirements for a secure agent-mediated application and highlights technical differences in platforms for autonomic computing. The research work also makes a contribution towards threat analysis techniques for autonomic applications and presents countermeasures and techniques for preventing various attacks from being launched by adversaries.

- Security in electronic commerce goes beyond platforms and application systems. Human agents that own and use these systems usually have special requirements such as privacy and self-determination. In Ssekibuule *et al.* [107] we make a contribution towards a secure secure publish-subscribe scheme that can be used in open-distributed environments for electronic commerce. This research work makes a novel contribution towards the use of cryptographic systems in applications of digital currency for untraceability or privacy and confidentiality.

- In Ssekibuule *et al.* [108] we contribute to the evaluation of techniques for preventing strategic liars in auction markets and electronic commerce systems in general. An evaluation of techniques for reputation mechanisms in electronic markets is done and a rating of their effectiveness presented. This research therefore contributes to the understanding of attacks on reputation mechanisms and techniques that are used by adversaries in electronic commerce environments to achieve their goals. The research work provides a platform for benchmarking security techniques for preventing shill attacks in autonomic electronic commerce environments.

Our research contributions can be classified in three system levels, namely; the platform level, application level and protocol level of application development.

7.4 Reflection on research limitations

We carried out the first pilot for the auction-market system in the first half of 2013. The pilot was executed in 4 districts of central Uganda, namely; Masaka, Bukomansimbi, Sembabule and Kalungu. During the first phase of piloting we were limited by financial resources to create a large scale awareness system for existence and presence of the system. Despite having reached a small number of early adopters, the word of mouth door-to-door awareness approach was not scaling to the numbers we desired. We registered less than 50 users with this approach and literally no market activity took place since most of the users were farmers, yet we also needed traders for transactions to take place.

We later on decided to use radio advertising with a local radio station which covered the central districts of Uganda. This approach got us about 1000 new users and consequently improved our transactional activities. The number of market matches subsequently improved but most of the matches did not turn into actual transactions exchanging money. We got only 13% of the market matches resulting into transactions exchanging funds. The limitation of these transactions resulted from the fact that the system was new and it was the first-of-the-kind SMS-based trading application. Many users were not sure whether they should commit their money to a new system yet several other had failed in the past. The radio adverts were few in number — we had a single 30 seconds advert once a week. Despite having got us more users than word-of-mouth advertising, we could have done better with a higher frequency of advertising.

The duration for once-a-week advertising was also short. We advertised for only 4 months and this did not create enough momentum for one thousand users to grow further on their own. We needed new market entrants to keep the asks and bids coming. Agricultural products are also seasonal; once farmer has sold their crop, they have to wait another 4 or 6 months to be able to trade again. We needed to have a steady market presence with radio advertising campaigns to bring on board new farmers and traders. We stopped advertising after we had run out of funds. The market activities went on decreasing for another 2 months and then we stopped collecting data in the third month.

7.5 Conclusions and future research work

The thesis has presented a threat model and an analysis of threats in the environment of software-agents and market entities participating an open distributed environment. We have presented the paradigm of software-agents in an automated agent-mediated negotiation framework and illustrated how threats in this environment evolve. We

have additionally presented security countermeasures to evolving security threats for agent-mediated solutions in an open distributed environment.

The current environment for agricultural trade in developing countries mostly relies on centuries old techniques to achieve exchange of market information leading to high levels of information asymmetry in the agricultural markets.

On the other hand we have market designs for other commodities in electronic markets that do not typically work well with agricultural markets in developing countries such as Uganda. The research work in this thesis has developed an agricultural market system which is appropriate for developing countries and also incentive compatible with existing rules of market engagements in order to drive participation.

As indicated in the general objective, research work in this thesis has contributed towards techniques necessary for developing secure and incentive compatible electronic-markets in developing countries. We have demonstrated appropriateness of our solution for electronic trade in agricultural produce through the two pilot launches that we carried out in central Uganda. We have observed that the design and implementation results are robust towards confidentiality, privacy and availability threats in a network environment.

The next phase of this research work shall mainly involve extending the clearing algorithm to specify more robust constraints for bids and asks in market submissions. The clearing algorithm will require integration of objective-functions to optimize buyer and seller constraints given standing market parameters. The current market-clearing algorithm performs distance measures between buyers and sellers using centroids between parishes, districts and subcounties. As much as centroid measures can be used to compute estimated distances between two locations, it is not a good measure for true road distance between two trading parties. It would be more desirable to implement a more reliable mechanism that depends on surveyed map of road networks such Google-Maps [109] or OpenStreetmap [110, 111].

The market environment currently does not enforce quality specification for produce since buyers and sellers currently follow a fair-average-quality. There is a need to grow the market to a national scale so that the market can gather enough momentum to push for standardized quality specifications across the country.

We experienced several malformed SMS messages during the two phases of piloting for the auction system. The next frontier of research activities need to investigate new approaches to predictive correction of SMS messages to reduce on the amount of manual effort required to correct wrongly formatted SMS messages. Another improvement related to user-interfacing is implementation and piloting of an Un-

structured Supplementary Service Data (USSD) to be used to provide a structured interface to end-users. USSD presents an interface to end-user with a trusted level of input validation. Unlike SMS, USSD provides a stepwise approach for buyers and sellers to submit their request to the market.

The planned USSD interface also has unknown variables which need to be analyzed. USSD interfaces have been used in East African countries of Kenya, Uganda and Tanzania to offer mobile-money services. These services are however supported by a large network of support agents. There is a need to investigate whether end-users with low-levels of literacy will be able to operate the auction-application on their own without a large network of support agents.

Appendix: Security Analysis of an Autonomic Application

A

This chapter presents a security analysis of an agent mediated application in an open distributed environment. We use a case study of a booktrading application that we implemented using AgentScape and JADE agent platforms. We analyze whether security requirements, threats and countermeasures for an agent mediated application change when implemented on different agent platforms and presents countermeasures to generic and application specific threats. In section A.1 we present an introduction to agent platform components which are pertinent to the development of agent-mediated applications, section A.2 presents a booktrading application as an example for agent-mediated applications. In section A.3 we present assets and components of an agent-mediated application which form a foundation for performing security analysis. Section A.4 presents security requirements for a secure agent-mediated application and section A.5 presents a threat model for the application. In section A.6 we present our experiences for developing the autonomic application and the conclusions. Section A.7 presents possible future work.

A.1 Introduction

Research and development in Agent system has seen tremendous progress in recent years leading to the development of several agent platforms such as NOMADS[112], AgentScape[33], Havana[113], JADE[114] and Aglets[115]. In order for agents to execute tasks that have been assigned to them, they have to interact with other agents in the open distributed environment whose intentions could be malicious. Several researchers [116, 117, 118] have suggested solutions to different types of threats that can be anticipated in agent-based applications and platforms. However, most of these solutions are based on generic analysis of threats and security countermeasures. Consequently, such solutions do not address specific application security requirements and threats. To address this problem, we perform security analysis using an agent-mediated case study and propose generic countermeasures to security threats based on a concrete application. The study also proposes an approach for performing systematic security analysis for agent-mediated application based on our

results and experiences. The chapter also investigates whether security requirements and threats change when an application is implemented using different types of agent platforms.

A.2 The booktrading application

The booktrading application comprises of booksellers and bookbuyer software agents that are ideally owned by separate individuals. The bookseller owners are responsible for maintaining bookstore operations which include stocking and setting prices for books. Bookbuyer software agents are responsible for buying books from bookseller agents on behalf of their owners. The implementation of the booktrading application was done in AgentScape[33] (version 0.9.1) and Java Agent Development Environment[114] (JADE version 3.6) agent platforms. The purpose of implementing the application in two agent platforms was to investigate whether threats, security requirements and threat countermeasures for the application would change when implemented in either of the platforms.

The bookseller interface is used by the bookseller owner to store information about books available for sale. In addition to the book title and year of book publication, the bookseller also records the first price of the book and lowest price at which he/she can sell a book. The first price is the best reasonable price that a seller finds competitive in the market. It is in the best interest of booksellers to keep information about the lowest price of the book secret from buyers and other sellers. Keeping this information secret, prevents the bookseller from being exploited by buyers during negotiation. Additionally, the bookseller might be helped in keeping pricing information secret from other booksellers to avoid competition that may arise from other booksellers in the environment setting their prices based on what they know about the seller.

The bookbuyer interface is used by the bookbuyer owner to send out requests to booksellers. Using the bookbuyer interface, the bookbuyer owner informs the agent of the best price at which they wish to buy the book and the maximum amount they are willing to pay. The bookbuyer agent also implements a protocol for negotiation with the bookseller in case the desired book is found to be at a price higher than the bookbuyer's best price. The current implementation of the negotiation protocol always proposes a price that is half the sum of the best and highest price. Ideally this strategy should not be known to the bookseller, otherwise a bookseller agent can exploit this information to sell at a higher price to the bookbuyer than they should have done in case they didn't know the buyer's negotiation strategy. Figure A.1 below presents an interaction protocol between the bookseller and bookbuyer for the booktrading application.

The current implementation of the booktrading application does not support mobility of either the bookseller or the bookbuyer. The choice of having the bookseller

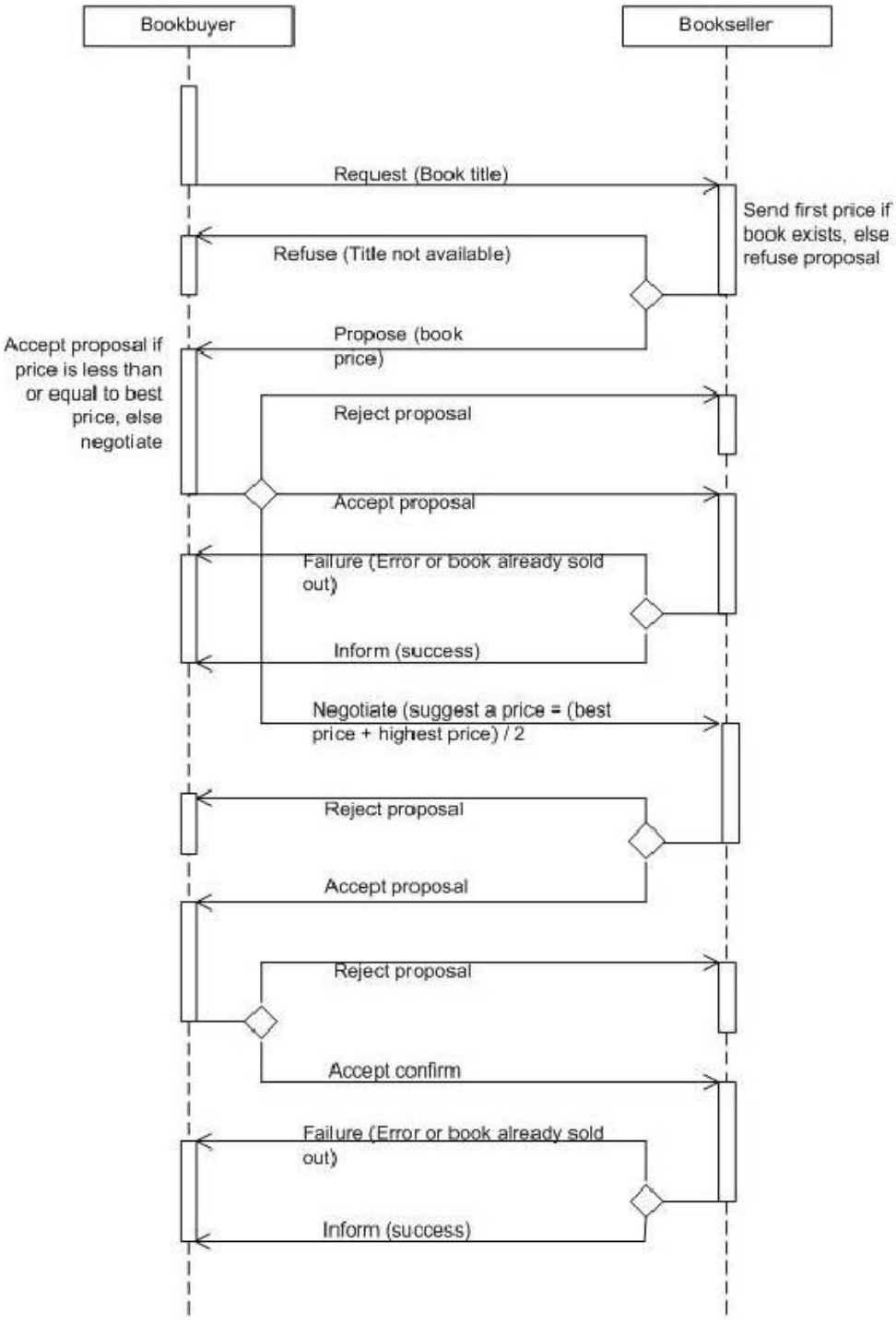


Fig. A.1.: *Interaction protocol for booktrading application*

stationary was a design decision made to support functionality for storing books in a MySQL[119] database, while the choice of having the bookbuyer stationary was due to limitations in inter-platform migration of JADE agents. The current version (3.6) of JADE does not have proper support for inter-platform migration. The mobility addon was developed for an older version of JADE and has not been since updated. Similar design decisions where taken with AgentScape, but the implementation limitations were different from those experienced with JADE. Nevertheless, security considerations for having the bookbuyer mobile were considered. The requirement of having the bookbuyer mobile could arise when it is deemed necessary to have the buyer migrate to the platform that has the desired book. Such a necessity would arise in case it is considered computationally expensive for the buyer to perform all tasks from the bookbuyer owner's platform.

A.3 Stakeholders and assets

This section presents stakeholders and assets in the booktrading application and agent platforms that were used in the implementation of the booktrading application. These stakeholders and assets are partly derived from the functional requirements of the booktrading application.

A.3.1 Booktrading application stakeholders

(i) ***Application creator:*** This is the individual or organization that developed both the agent bookseller and agent bookbuyer. (ii) ***Bookseller owner:*** The individual or organization that owns the bookseller agent. (iii) ***Bookbuyer owner:*** The individual or organization that owns the bookbuyer agent. (iv) ***Platform creator:*** The individual or organization that developed the agent middleware (here in referred to as the agent platform). (v) ***Platform owner:*** This is the stakeholder category that owns or administers the operating system (host) on which the agent platform is installed

A.3.2 Booktrading application assets

Bookseller agent: This is the agent code that is responsible for handling tasks related to storing books in the bookstore and interacting with bookbuyers.

Bookbuyer agent: The agent code that represents the human bookbuyer in booktrading tasks. The bookbuyer agents captures the title, the maximum age of the book, best and highest price that the agent owner would be willing to pay for the book.

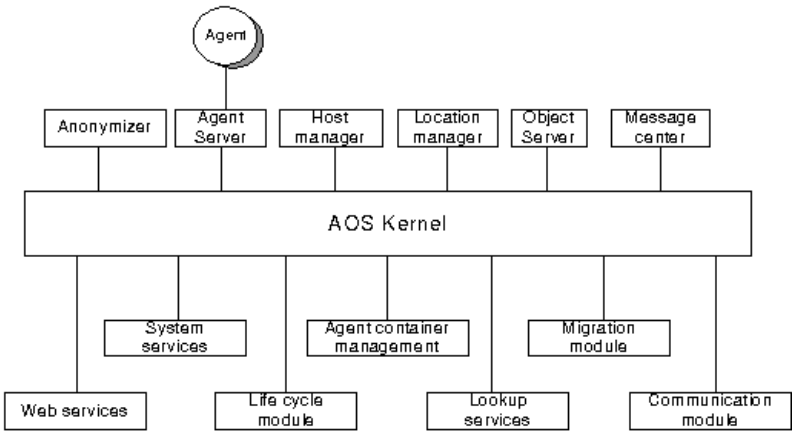


Fig. A.2.: *AgentScape Architecture*

Interaction protocol: The interaction protocol represents a set of rules through which messages exchanged between the agent buyer and agent seller are interpreted. In case the interaction protocol is is not followed, it is assumed that either party would not understand what they other is saying. The format of interaction messages were previous defined by Foundation of Intelligent Physical Agents (FIPA)[16]. The booktrading application extends the interaction protocol to include negotiation. The negotiation protocol is implemented by the bookseller and bookbuyer agents to handle the logic through which they can agree on an alternative price that is different from the booksellers first price and the bookbuyers best price.

Agent platform: The agent platform provides the execution environment for both the bookseller and bookbuyer.

A.3.3 Platform assets

This section presents platform assets for AgentScape and JADE agent platforms. Separating the assets and possible attacks to the agent platforms created a basis for thinking about generic countermeasures for attacks on agent platforms.

AgentScape platform assets

AgentScape system services: (The component represents core kernel services for AgentScape. System services ensure that the right classes are used in the communicator. AgentScape system services provide lookup services through which agents and services are registered and discovered. They also provide a communication module through which messages are exchanged between agents and remote agent management platforms.

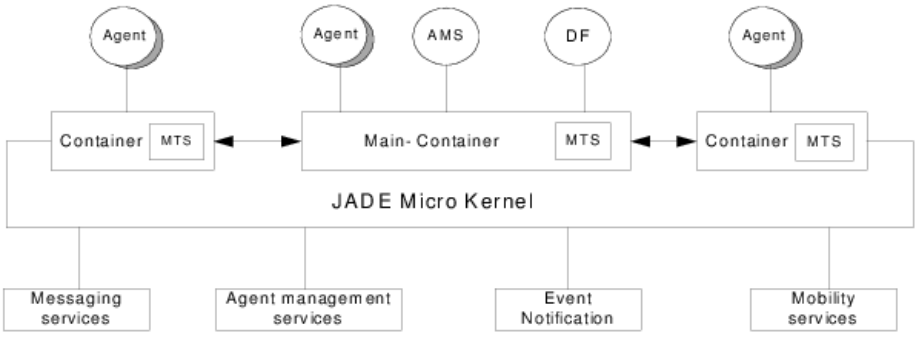


Fig. A.3.: *JADE Platform Architecture*

Agent server: Provides services for loading of agent code from the agent container, startup and termination of the agent. Facilitates agent access to kernel services, provides mechanism for making negotiation calls. The agent server also uses an agentwrapper to provide interaction between a running agent and agentscape middleware.

Host manager: AgentScape host manager provides agent container management for mediating access to agent stores. The hostmanager additionally facilitates data handling during agent migration. The host manager provides agent life cycle management services such as migration, suspending, stopping and running of an agent.

Location manager: Provides an agent management module that facilitates inserting new agents into a location and handling of migration requests from local agents and remote location managers.

Jade Platform Assets

JADE Core Base Service: Microkernel of the JADE system that provides a uniform mechanism for management and service discovery.

Agent Management Services: Agent management services define the agent, provide platform administration, status information for agents and a unique naming scheme.

Messaging Services: Microkernel service responsible for managing communication between agents and other entities in across agent platforms

Event Notification Services: Represents events related to the agent life-cycle and configuration.

Agent Mobility Services: JADE microkernel provides an agent mobility service to facilitate migration within containers on the same platform and migration from one platform to another.

A.4 Security requirements

This section covers security requirements for both the agent platform on which the agent-mediated application can be executed and security requirements for the booktrading application.

A.4.1 Application security requirements

We use the Confidentiality, Integrity, Authentication and Non-repudiation (CIAN) taxonomy to define security requirements for both the bookseller and bookbuyer agents. The Confidentiality, Integrity and Authentication (CIA) taxonomy has been reviewed by Howard et. al [120] in regard with risk analysis. This section presents a forth requirement of non-repudiation and brief definition of CIA components.
Confidentiality: This is a security requirement that ensures information exchanged and stored in the system is accessed by only authorized users. ***Integrity:*** This requirement ensures that changes to information or application code are only done by authorized users. ***Availability:*** This is a security requirement that ensures that information and application resources can be accessed by all legitimate parties. The legitimate parties may include users and software processes. ***Non-repudiation:*** This security requirement ensures that all parties can be held accountable for their actions. It ensures that all actions taken cannot be denied at a later time.

A.4.2 Bookseller security requirements

This subsection presents security requirements for the bookseller agent application.

Confidentiality: The bookseller should not release buyers private information to the public and the information should be protected from attackers.

Integrity: Bookseller should prevent book reviews from being manipulated or changed by people who did not write them.

Availability: (i) The bookseller should not prevent some books from being available to some buyers for one reason or another. (ii) The bookseller should allow the buyer to choose a book based on attributes such as price, publication date, quality and relevance among others. (iii) The bookseller should not deny bookbuyers a chance to negotiate when requested. (iv) The bookseller should not disable possibilities of

writing reviews and posting them from genuinely critical reviewers and buyers. (v) The bookseller should not prevent potential buyers from reading book reviews.

Non-repudiation: The bookseller should not be able to deny any information that is exchanged with the bookbuyer such as having received payment from bookbuyers or purchase orders.

A.4.3 Bookbuyer security requirements

This subsection presents security requirements for the bookbuyer agent application.

Confidentiality: (i) Should be able to migrate from one platform to another and perform computational tasks from local and remote hosts/platforms without leaving information traces for attackers. Such information could include platforms/hosts they have previously visited and budget information for their shopping. (ii) The bookbuyer should have control on the type of information that they have to submit to the operation environment. Withholding some information for privacy reasons should not be a cause for denying them access to requested services. (iii) Bookbuyer should avoid forming a coalition in which it will be exploited. E.g exposing information it carries to malicious bookbuyers.

Integrity: (i) The bookbuyer should not be manipulated to buy a book that is not the best on offer. (ii) The information carried by the bookbuyer agent on behalf of the agent owner, should be protected from attackers that might want to change it.

Availability: (i) Bookbuyer should be able to find a book available for sale. (ii) The bookbuyer agent should protect the information it carries and prevent it from being destroyed by attackers. (iii) Bookbuyer should not be prevented from forming a coalition with other bookbuyers for mutual benefit.

Non-repudiation: The bookbuyer should not be able to deny that they ever ordered for a book.

A.4.4 Platform security requirements

The agent platform security requirements are derived from the CIAN acronym that was defined in subsection A.4.1.

Confidentiality: In case of agent migration, the agent platforms needs to protect the migration path of the agent. The migration path might contain information concerning platforms the agent has previously visited and intended destinations.

Integrity: (i) The agent platform is expected to maintain integrity of agents (agent code) and protect them from malicious attackers in the environment. It is important to note that malicious platforms might try to do otherwise. (ii) The agent platform should provide a mechanism for detecting compromised or malicious agents.

Availability: (i) The agent platform needs to ensure availability of messaging service for agent communication. Termination of the messaging service would prevent agents from communicating, while a comprised messaging service could yield unexpected and undesired results for the intentions of the communication. For example, attacker could delay messages for the intended destination whose requests might have been time bound. (ii) The agent platform should have policies for regulating access to system resources to prevent starvation of some agents by others that may intentionally or otherwise over consume system resources.

Non-repudiation: The agent platform needs to provide a mechanism through which agents can be accountable for the actions they perform when visiting platforms.

A.5 Threat modeling

We use the STRIDE[120] taxonomy to identify possible threats faced by the book-trading application and the agent platform on which the application is executed.

Spoofing Identity: This is a form of attack in which someone or an entity pretends to be someone else of another entity. For example agent X pretending to be agent Y.

Tampering : Tampering attack refers to unauthorized changing of software code or information.

Repudiation: This refers to a circumstance in which a software process or an individual deny responsibility for their actions.

Information disclosure: This refers to unauthorized access to information.

Denial of Service: This is a form of attack that denies legitimate access to resources such as information, storage space, processor and communication channels.

Elevation of privileges: This refers to a form of attack in which an entity with lower privileges gains unauthorized higher privileges.

A more detailed explanation of the STRIDE components was presented by Howard et. al [120].

A.5.1 Application threat model

The book trading application is an agent mediated application in which one agent acts as a seller and another agent as a buyer. The bookseller agent provides a variety of books for sale in a manner similar to bookstores such as amazon, but in this setting the bookseller expects the buyers to be software agents. The bookbuyer agents are supposed to search in the books catalogue and compare prices and other attributes such as publication date, relevance and book ratings on behalf of their owners. The bookbuyer agent is expected to perform these tasks for a range of booksellers that have books available for sale. This section covers possible goals of the attacker against the bookseller and bookbuyer agents and suggests possible countermeasures to the identified threats.

Possible goals of attackers against bookseller

i. ***Spoofing Identity:*** An attacker could spoof the identity of a bookseller and requests payment from buyers for books that will not be delivered.

ii. ***Tampering:*** (i) The attacker may want to change information in the booksellers catalogue so that book attributes such as price, publication date, quality and relevance are not correct. These changes could lead bookbuyers into choosing items that they were not supposed to buy. (ii) An attacker could change book reviews and rating so that consumers will not buy books from that particular bookseller.

iii. ***Repudiation:*** A malicious bookbuyer could deny having requested or received a book from the bookseller.

iv. ***Information Disclosure:*** (i) The attacker could compromise the negotiation logic implemented in the bookseller. E.g. if an attacker knows the price that a consumer wishes to pay for a product, the attacker could lower their prices to out-compete other sellers or simply to distract the buyer from making a genuine negotiation or purchase. (ii) An attacker may wish to access and log information concerning bookbuyers. The intention of this attack would be to compromise buyers' privacy.

v. ***Denial of Service:*** (i) An attacker could block the messaging service between the bookbuyer and the bookseller. (ii) The attacker could try to remove items from the bookseller's catalogue of books so that books requested by the bookbuyer are not available. (iii) An attacker could block buyers from writing and sending reviews on books. Such an attack could negatively affect the

bookseller if buyers wish to know whether the books on sale are good and price worthy.

Possible goals of attackers against bookbuyer:

i. ***Spoofing Identity:*** An attacker could spoof the identity of a bookbuyer agent and purchases books that could be reputation damaging to the agent owner. This attack could be more severe in a general purpose e-commerce application where many types of products could be bought.

ii. ***Tampering:*** (i) The attacker could alter message responses from the bookseller to indicate to the bookbuyer that the requested book is not available, even when it is actually available. (ii) An attacker could change book reviews and rating so that consumers are lured into buying books that are not price worthy. (iii) An attacker could change information requests from the bookbuyer to indicate different requests to the bookseller from the ones submitted by the bookbuyer. Such attacks could lead the bookbuyer into getting invoices for books they did not order. Additionally, buyers could get false responses such as requested books not being available, even in circumstances where the books are available.

iii. ***Repudiation:*** A malicious bookseller could deny having received payment for a book. In such a case, the bookbuyer would end up losing money.

iv. ***Information Disclosure:*** (i) An attacker may have interest in accessing private information that is carried by a bookbuyer agent. (ii) An attacker could lure a bookbuyer into forming a coalition in which it would be exploited. E.g leaking information it carries to malicious bookbuyers.

v. ***Denial of Service:*** (i) An attacker could lure a bookbuyer into forming a coalition in which it would be exploited. (ii) The attacker could block the messaging service between the bookbuyer and the bookseller. (iii) The bookbuyer could be denied a chance of forming a coalition with other buyers by withholding coalition formation information. This attack could also affect the bookseller by not making a needed sale. (iv) An attacker could prevent potential buyers from reading book reviews. (v) An attacker could create a malicious bookstore to prevent a bookbuyer from finding a genuine book to buy.

Application specific countermeasures

This section presents countermeasures for the security challenges that are likely to be faced by the agent bookseller and bookbuyer. The countermeasures are meant to

prevent attackers' goals that were identified in subsection A.5.1. The countermeasures are combined for attacks on the bookseller and bookbuyer agents, because these attacks are similar in nature. We also assume that safe coding procedures were followed for both the application and agent platform. When software security flaws such as buffer overflows exist in software, then authentication and authorization schemes can be subverted.

i. ***Spoofing Identity:*** Spoofing of an agent's identity can be prevented by providing an identity management system[121] through which agents are assigned names (or identities) that are difficult to be changed by the agent or an attacker. Authentication and authorization systems such as kerberos[122] or message authentication codes [123] can be used to authenticate agents' identity or their owners. In this setup an agent would be required to submit a message to the service provider indicating their identity and a small message encrypted by their private key. The service provider would then retrieve a public key (from the key-management system) that is needed to decrypt the short message. It is assumed with public-key cryptography that the private key of the agent is key secret.

ii. ***Tampering:*** Two things need to be protected against tampering. That is the information or data carried by agents and the agent code. The countermeasures available against these attacks fall into categories of prevention and detection. Message authentication codes (MAC)[123] and digital signatures on the agent code and data are used to detect any form of tampering on the agent code and data.

iii. ***Repudiation:*** Public-key digital signatures can be used to prevent repudiation by either a malicious bookseller or bookbuyer. In order to prevent repudiation, digital signatures would be required on messages from either the bookbuyer or bookbuyer. When a given agent (A) encrypts messages using their private key, those messages can only be decrypted by a corresponding public key that certainly belongs to the sending agent. The main challenge to this kind of solution is that security depends on the secrecy of the secret key.

iv. ***Information Disclosure:*** This countermeasure should protect information carried by the agent. Such information includes target book titles, best and highest price that the bookbuyer is willing to pay for the book. Confidentiality of this information can be provided by encrypting the information carried by agents.

v. ***Denial of Service:*** The agent platform and agent execution environment needs to provide strong authentication[122] and authorization for processes

that access system resources. Authentication and authorization are useful in preventing non-authorized users and processes from accessing privileged resources that could be critical for correct functionality of the agent application. Apart from preventing users and processes from accessing privileged resources and services, authentication is useful for detecting users and processes that may breach the imposed restriction. In detecting which users or processes performed certain tasks, accountability can be achieved for all activities undertaken in the system. The concept of a trusted third party can be used to determine ratings of a bookseller before it can be considered by the book-buyer for purchase of a book. A trusted third party would help in preventing malicious booksellers from participating in booktrading transactions.

A.5.2 Platform threat model

The platform threat model is based on the Java Agent Development Environment (JADE)[124] and AgentScape[33] platforms whose assets were presented in subsections A.3.3 and A.3.3 respectively.

Possible goals of attackers against agent platform

i. ***Spoofing Identity*** An attacker could launch counterfeit agents using the agent platform to participate in a transaction they are not supposed to be involved. For example, an agent Z (representing an attacker) could spoof the identity of agent X in order to perform actions privileged to X.

ii. ***Tampering*** (i) An attacker could be interested in altering agent code through the agent platform so that the agent does not do what it is supposed to do. (ii) The attacker could use a weakness in the agent platform to reach and subvert the communication channel for agents. (iii) The attacker could use the platform to migrate an agent from a trusted platform to a compromised one.

iii. ***Information Disclosure***

In circumstances where agent platforms keep a non-repudiable log of agent events, an attacker could be interested in knowing about action of a particular agent. An attacker accessing this information could violate agent's confidentiality requirements. Additionally, the attacker could use this information to launch other forms of attacks against the agent.

iv. ***Denial of Service*** An attacker could be interested in subverting the Agent Management System (AMS), Directory Facilitator (DF) and Management services.

v. ***Elevation of Privileges*** Exploiting a flaw in the agent platform to grant higher privileges to malicious agents. Such malicious agents could be interested in using free resources on platform hosts, or even over-consuming system resources in order to deny services to legitimate users

Platform specific countermeasures

This section presents security techniques that are needed by the platform to achieve the security requirements indicated in section A.4.4 and to prevent attackers from achieving their objectives stated out in subsection A.5.2.

i. ***Spoofing Identity:*** Provide identity management: Only authenticated and registered agent owners are allowed to launch booksellers into the environment to prevent scenarios of malicious booksellers. A trusted third party can be used to verify and certify credentials agents.

ii. ***Tampering:*** As indicated in subsection A.5.2 the attacker may want to change the agent code or migrate an agent to a malicious platform. The action of changing or tampering with agent code can be prevented by code signing [118] with a digital signature. Agent migration to malicious platforms can prevented by use of security policies to authorize sensitive actions to be executed by only trusted parties.

iii. ***Repudiation:*** Combined with identity management, a non repudiable log kept by the agent platforms would be useful in tracking actions that were performed by various agents.

iv. ***Information Disclosure:*** Confidentiality of the agent logs resident on the agent platform can be achieve through encryption. However, encryption has to be applied with consideration for low resource platforms like mobile devices.

v. ***Denial of Service:*** Use of security policies for authentication and authorization of users and processes to key assets for the agent platform would prevent denial of service attacks.

vi. ***Elevation of Privileges:*** This attack can be stopped by preventing software security flaws such as buffer overflows and SQL injection. Language based security mechanisms such as static source code analysis to enforce safety properties of the programming language, sand-boxing and proof carrying code can be used.

A.6 Conclusions and remarks

In this chapter, we present a systematic approach for performing a security analysis of an agent mediated application. We have presented the Confidentiality, Integrity, Availability and Non-repudiation (CIAN) framework through which security requirements for an application can be derived and combined it with STRIDE[120] to obtain possible attacker goals. The proposed countermeasures (presented in subsections A.5.2 and A.5.1) are clearly generic for any agent application and indicate generic assets that need to be protected in an agent mediated application.

Our results indicate that security requirements for the agent application did not change significantly when implemented with either AgentScape or JADE. In reference to subsection A.3.3, the assets of the agent platforms fall in the categories of (i)*Agent Management Services*, (ii) *Directory Facilitator*, (iii) *Messaging Services*, (iv) *Mobility Services* and (v) *Event Notification Services*. This implies that these assets need to be protected irrespective of the agent platform against all possible forms of attacks for the agent environment to be considered secure. Furthermore, for any application to be considered secure, its security requirements have to be catered for in the implementation and assets protected.

A.6.1 Implementation experiences and challenges

This section presents some key issues and experiences that were encountered during the implementation phase of the booktrading application on JADE and AgentScape platform.

The implementation challenges were different for the platforms (AgentScape and JADE) that were used. Intra-platform migration challenges were faced with JADE (version 3.5 and 3.6) mainly because the mobility add-on was implemented for lower version of JADE. In AgentScape, implementation challenges were faced with service discovery facility due to the nature of requirements that were imposed by the application. It is worthy noting that these middleware platforms (mostly especially AgentScape) are still under heavy development and most problems are being solved as they are reported by users.

A.7 Future work

The information disclosure countermeasure needs to protect the bookbuyer against traffic analysis by an intelligent bookseller. In this example booktrading application, the bookbuyer negotiates by sending a second price that is half the sum of the best

and highest price. Using traffic analysis, an intelligent bookseller could be able to generate these two (best and highest) prices of the bookbuyer. The bookseller knowing these prices puts the bookbuyer in a poor negotiation position. Furthermore, the countermeasure should protect the negotiation protocol from revealing negotiation strategy. Additionally, some malicious participants could start the negotiation protocol and then terminate it with the intentions of stealing information concerning pricing and introducing annoyance attacks.

List of Figures

List of Tables

Curriculum Vitae

Born on 10th April 1979, Kampala, Uganda

Academic

- 1999 - 2002: Makerere University (Bachelor of Science, Computer Science & Mathematics)
- 2004 - 2006: Radboud University (Master of Science, Computer Science)
- 2009 - 2016: Radboud University (PhD Computer Science)

- 2003 - 2004: Makerere University (Teaching Assistant)
- 2006 - Now: Makerere University (Assistant Lecturer)

Industrial Experience:

- 2003 - 2004: Uganda Telecom (Billing Systems Administrator)
- 2008 - 2012: College of Computing and IT, Makerere University (Head ICT)
- 2014 - Now: dfcu Bank (Lead Systems Architect)

Bibliography

[1] C. Barrett and E. Mutambatsere, "Agricultural markets in developing countries," *The New Palgrave Dictionary of Economics, 2nd edition*, 2005.

[2] A. Lo, "Efficient markets hypothesis," *The new palgrave: A dictionary of economics*, 2007.

[3] M. Gakuru, K. Winters, and F. Stepman, "Inventory of innovative farmer advisory services using ICTs," Forum for Agricultural Research in Africa (FARA), Accra, GH, 2009.

[4] National Agricultural Advisory Services Programme, "Facts and Figures," *NAADs Uganda*, August.

[5] Central Intelligence Agency, "The World Factbook : Uganda," Accessed December 2012.

[6] R. Jensen, "Information, efficiency, and welfare in agricultural markets," *Agricultural Economics*, vol. 41, pp. 203–216, 2010.

[7] A. Reda, Q. Duong, T. Alperovich, B. Noble, and Y. Haile, "Robit: an extensible auction-based market platform for challenged environments," in *Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development*, ICTD '10, (New York, NY, USA), pp. 39:1–39:10, ACM, 2010.

[8] A. Reda, B. Noble, and Y. Haile, "Distributing private data in challenged network environments," in *Proceedings of the 19th international conference on World wide web*, pp. 801–810, ACM, 2010.

[9] P. Bogetoft, D. L. Christensen, I. Damgård, M. Geisler, T. Jakobsen, M. Krøigaard, J. D. Nielsen, J. B. Nielsen, K. Nielsen, J. Pagter, *et al.*, "Secure multiparty computation goes live," in *Financial Cryptography and Data Security*, pp. 325–343, Springer, 2009.

[10] Y. Shoham and K. Leyton-Brown, *Multiagent systems: Algorithmic, game-theoretic, and logical foundations*. Cambridge University Press, 2008.

[11] J. W. Creswell, "The selection of a research approach," *Chapter One*, vol. 1, pp. 3–21, 2014.

[12] Famine Early Warning Systems Network, "Uganda Monthly Price Bulletin," September 2010.

[13] S. Ilieva, P. Ivanov, and E. Stefanova, "Analyses of an agile methodology implementation," in *Euromicro Conference, 2004. Proceedings. 30th*, pp. 326–333, IEEE, 2004.

[14] L. M. Maruping, V. Venkatesh, and R. Agarwal, "A control theory perspective on agile methodology use and changing user requirements," *Information Systems Research*, vol. 20, no. 3, pp. 377–399, 2009.

[15] USAID Mission to Uganda, "Moving from Subsistence to Commercial Farming in Uganda," *http://pdf.usaid.gov/pdf_docs/PDACM231.pdf*, June 2008.

[16] F. FIPA, "Contract Net Interaction Protocol Specification," 2002.

[17] D. Kreps, "Arbitrage and equilibrium in economies with infinitely many commodities* 1," *Journal of Mathematical Economics*, vol. 8, no. 1, pp. 15–35, 1981.

[18] R. Ferris, P. Engoru, M. Wood, and E. Kaganzi, "Evaluation of the market information services in uganda and recommendations for the next five years," *Contract for PMA/ASPS. Danish Embassy, Kampala, Uganda*, 2006.

[19] N. Jennings, "An agent-based approach for building complex software systems," *Communications of ACM*, vol. 44, no. 4, pp. 35–41, 2001.

[20] M. He, N. Jennings, and H. Leung, "On agent-mediated electronic commerce," *IEEE Transactions on Knowledge and Data Engineering*, vol. 15, no. 4, pp. 985–1003, 2003.

[21] M. Wooldridge and N. Jennings, "Intelligent Agents: Theory and Practice," *Knowledge Engineering Review*, vol. 10, no. 2, pp. 115–152, 1995.

[22] K. Sycara, "Multiagent Systems," *AI Magazine*, vol. 19, no. 2, pp. 79–92, 1998.

[23] L. Molm, N. Takahashi, and G. Peterson, "Risk and Trust in Social Exchange: An Experimental Test of a Classical Proposition," *AJS*, vol. 105, no. 5, pp. 1396–1427, 2000.

[24] S. Ramchurn, D. Huynh, and N. Jennings, "Trust in multi-agent systems," *The Knowledge Engineering Review*, vol. 19, no. 01, pp. 1–25, 2005.

[25] R. Guttman, A. Moukas, and P. Maes, "Agent-mediated electronic commerce: a survey," *The Knowledge Engineering Review*, vol. 13, no. 02, pp. 147–159, 2001.

[26] P. Maes, R. Guttman, and A. Moukas, "Agents that buy and sell: Transforming commerce as we know it," *Communications of the ACM*, vol. 42, no. 3, 1999.

[27] R. Glushko, J. Tenenbaum, and B. Meltzer, "An XML framework for agent-based E-commerce," *Communications of the ACM*, vol. 42, no. 3, 1999.

[28] N. Gibbins, S. Harris, and N. Shadbolt, "Agent-based Semantic Web Services," *Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 1, no. 2, pp. 141–154, 2004.

[29] M. Filzmoser and R. Vetschera, "A Classification of Bargaining Steps and their Impact on Negotiation Outcomes," *Group Decision and Negotiation*, vol. 17, no. 5, pp. 421–443, 2008.

[30] N. Jennings, P. Faratin, A. Lomuscio, S. Parsons, M. Wooldridge, and C. Sierra, "Automated negotiation: prospects, methods and challenges," *Group Decision and Negotiation*, vol. 10, no. 2, pp. 199–215, 2001.

[31] C. Bartolini, C. Priest, and N. Jennings, "A software framework for automated negotiation," *Software Engineering for Multi-Agent Systems III: Research Issues and Practical Applications*, pp. 213–235, 2005.

[32] D. Mobach, *Agent-Based Mediated Service Negotiation*. Phd thesis, 2007.

[33] B. Overeinder and F. Brazier, "Scalable Middleware Environment for Agent-Based Internet Applications," *Lecture Notes in Computer Science*, vol. 3732, p. 675, 2005.

[34] J. Collins, W. Ketter, and M. Gini, "A multi-agent negotiation testbed for contracting tasks with temporal and precedence constraints," *International Journal of Electronic Commerce*, vol. 7, no. 1, pp. 35–57, 2002.

[35] J. Collins and M. Gini, "MAGNET: A Multi-Agent System using Auctions with Temporal and Precedence Constraints," *Multiagent based Supply Chain Management*, pp. 273–314, 2006.

[36] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[37] R. Al-Jaljouli and J. Abawajy, "Secure Mobile Agent-based E-Negotiation for On-Line Trading," *IEEE International Symposium on Signal Processing and Information Technology*, pp. 610–615, 2007.

[38] R. Al-Jaljouli and J.H., "Electronic Negotiation and Security of Exchanged Information in e-Commerce," tech. rep.

[39] L. Moreau, "Distributed directory service and message routing for mobile agents," *Science of Computer Programming*, vol. 39, no. 2-3, pp. 249–272, 2001.

[40] A. Jaiswal, Y. Kim, and M. Gini, "Design and implementation of a secure multi-agent marketplace," *Electronic Commerce Research and Applications*, vol. 3, no. 4, pp. 355–368, 2004.

[41] C. Farkas, G. Ziegler, A. Meretei, and A. Lörincz, "Anonymity and accountability in self-organizing electronic communities," in *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, pp. 81–90, 2002.

[42] G. Ziegler, C. Farkas, and A. Lőrincz, "A framework for anonymous but accountable self-organizing communities," *Information and Software Technology*, vol. 48, no. 8, pp. 726–744, 2006.

[43] M. Warnier and F. Brazier, "Anonymity Services for Multi-Agent Systems," *An International Journal In Web Intelligence and Agent Systems*, 2009.

[44] R. Rivest, A. Shamir, and D. Wagner, "Time-lock puzzles and timed-release crypto," 1996.

[45] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," tech. rep., August 2008.

[46] M. Warnier, M. Oey, R. Timmer, F. Brazier, and B. Overeinder, "Enforcing integrity of agent migration paths by distribution of trust," *International Journal of Intelligent Information and Database Systems*, 2008.

[47] A. Saxena and B. Soh, "Authenticating mobile agent platforms using signature chaining without trusted third parties," in *IEEE International Conference on e-Technology, e-Commerce and e-Service*, pp. 282–285, 2005.

[48] A. Balogh, F. Brazier, R. Hofman, A. Tanenbaum, and G. Noordende, "A Secure Jailing System for Confining Untrusted Applications," *2nd International Conference on Security and Cryptograpy*, 2007.

[49] R. Sekar, V. Venkatakrishnan, S. Basu, S. Bhatkar, and D. DuVarney, "Model-carrying code: A practical approach for safe execution of untrusted applications," in *ACM symposium on operating systems principles*, p. 28, ACM, 2003.

[50] G. Necula, "Proof-carrying code," in *ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, pp. 106–119, 1997.

[51] T. Quillinan, M. Warnier, M. Oey, R. Timmer, and F. Brazier, "Enforcing security in the AgentScape middleware," in *Workshop on Middleware security*, pp. 25–30, ACM, 2008.

[52] S. Tomas and F. Tschudin Christian, "Protecting mobile Agents against malicious hosts," *Mobile Agent Security, Spring-Verlag*, 1998.

[53] V. Gunupudi and S. Tate, "SAgent: A security framework for JADE," in *International joint conference on Autonomous agents and multiagent systems*, p. 1118, 2006.

[54] V. Roth and M. Jalali, "Concepts and architecture of a security-centric mobile agent server," in *International Symposium on Autonomous Decentralized Systems*, pp. 435–442, 2001.

[55] A. Helsinger, M. Thome, and T. Wright, "Cougaar: a scalable, distributed multi-agent architecture," in *IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, pp. 1910–1917, 2004.

[56] Dynamic Adaptive Systems Design Group, "Agentscape: Distributed agent middleware," *http://www.agentscape.org/*, 2013.

[57] F. Brazier, D. Mobach, B. Overeinder, E. Posthumus, S. v. Splunter, M. v. Steen, and N. Wijngaards, "Agentscape demonstration," in *Proceedings of the Fourteenth Belgium-Netherlands Conference on Artificial Intelligence (BNAIC2002)* (H. Blockeel and M. Denecker, eds.), pp. 513–514, October 2002.

[58] K. Fullam, T. Klos, G. Muller, J. Sabater, A. Schlosser, Z. Topol, K. Barber, J. Rosenschein, L. Vercouter, and M. Voss, "A specification of the Agent Reputation and Trust (ART) testbed: experimentation and competition for trust in agent societies," in *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, p. 518, ACM, 2005.

[59] W. Shi, I. Jang, and H. Yoo, "An Efficient Electronic Marketplace Bidding Auction Protocol with Bid Privacy," *Lecture Notes in Computer Science*, vol. 4976, pp. 297–308, 2008.

[60] R. Guttman, A. Moukas, and P. Maes, "Agent-mediated electronic commerce: A survey," *The Knowledge Engineering Review*, vol. 13, no. 02, pp. 147–159, 2001.

[61] P. Maes, R. Guttman, and A. Moukas, "Agents that buy and sell," 1999.

[62] A. Shikfa, M. Onen, and R. Molva, "Privacy-Preserving Content-Based Publish-Subscribe Networks," in *Emerging Challenges for Security, Privacy and Trust: 24th Ifip Tc 11 International Information Security Conference, SEC 2009, Pafos, Cyprus, May 18-20, 2009, Proceedings*, p. 270, Springer, 2009.

[63] A. Shamir, "On the power of commutativity in cryptography," *Automata, Languages and Programming*, pp. 582–595, 1980.

[64] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over GF (p) and its cryptographic significance (Corresp.)," *IEEE Transactions on information Theory*, vol. 24, no. 1, pp. 106–110, 1978.

[65] A. Carzaniga, D. Rosenblum, and A. Wolf, "Design and evaluation of a wide-area event notification service," *ACM Transactions on Computer Systems (TOCS)*, vol. 19, no. 3, pp. 332–383, 2001.

[66] C. Raiciu and D. Rosenblum, "Enabling confidentiality in content-based publish/subscribe infrastructures," *Securecomm and Workshops, 2006*, pp. 1–11, 2006.

[67] Ł. Chmielewski and J. Hoepman, "Fuzzy private matching," in *The Third International Conference on Availability, Reliability and Security, ARES*, pp. 327–334, Citeseer, 2008.

[68] N. Provos and N. Provos, "Preventing Privilege Escalation," in *Proceedings of the 12th USENIX Security Symposium*, 2003.

[69] B. C. Neuman and T. Ts' O, "Kerberos: An authentication service for computer networks," *Communications Magazine, IEEE*, vol. 32, no. 9, pp. 33–38, 1994.

[70] N. Mathewson, P. Syverson, and R. Dingledine, "Tor: the second-generation onion router," in *the Proceedings of the 13th USENIX Security Symposium*, 2004.

[71] I. Damgård, "A design principle for hash functions," in *Advances in Cryptology—CRYPTO'89 Proceedings*, pp. 416–427, Springer.

[72] S. Alexander, "Improving security with homebrew system modifications," *USENIX*, vol. 29, no. 6, pp. 26–32, 2004.

[73] N. Provos and D. Mazieres, "MD5-crypt," *USENIX*, 1999.

[74] N. Provos and D. Mazieres, "A future-adaptable password scheme," in *Proceedings of the Annual USENIX Technical Conference*, Citeseer, 1999.

[75] N. Provos and D. Mazieres, "Bcrypt," *USENIX*, 1999.

[76] H. Gilbert and H. Handschuh, "Security analysis of SHA-256 and sisters," in *Selected Areas in Cryptography*, pp. 175–193, Springer, 2003.

[77] E. Fleischmann, C. Forler, and M. Gorski, "Classification of the SHA-3 Candidates," *International Association for Cryptologic Research (IACR) ePrint archive*.

[78] J. Rushby, "A trusted computing base for embedded systems," in *Proceedings 7th DoD/NBS Computer Security Conference*, pp. 294–311, Citeseer, 1984.

[79] V. Costan, L. F. Sarmenta, M. Van Dijk, and S. Devadas, "The trusted execution module: Commodity general-purpose trusted computing," in *Smart Card Research and Advanced Applications*, pp. 133–148, Springer, 2008.

[80] M. Howard, D. LeBlanc, and J. Viega, *19 deadly sins of software security*. McGraw-Hill/Osborne, 2005.

[81] A. Blyth, "Secure coding–principles and practices," *Infosecurity Today*, vol. 1, no. 3, p. 46, 2004.

[82] O. David-West, "Esoko networks: facilitating agriculture through technology," *New York: United Nations Development Project*, 2011.

[83] K. V. Rao, "Rml: market intelligence in india with mobile sms intervention," *Emerald Group Publishing Limited*, 2011.

[84] J. Donner, "Mobile-based livelihood services in Africa: pilots and early deployments," *Communication technologies in Latin America and Africa: A multidisciplinary perspective*, pp. 37–58, 2009.

[85] M. J. Bixler and T. F. Trader, "Electronic classified advertising interface method and instructions with continuous search notification," Apr. 28 1998. US Patent 5,745,882.

[86] M. Fafchamps and B. Minten, "Impact of sms-based agricultural information on indian farmers," *The World Bank Economic Review*, vol. 26, no. 3, pp. 383–414, 2012.

[87] D. Friedman, "The double auction market institution: A survey," *The Double Auction Market: Institutions, Theories, and Evidence*, pp. 3–25, 1993.

[88] C. Dellarocas, "Reputation mechanisms," *Handbook on Economics and Information Systems*, 2005.

[89] D. Gregg and J. Scott, "The role of reputation systems in reducing on-line auction fraud," *International Journal of Electronic Commerce*, vol. 10, no. 3, pp. 95–120, 2006.

[90] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007.

[91] T. Huynh, N. Jennings, and N. Shadbolt, "An integrated trust and reputation model for open multi-agent systems," *Autonomous Agents and Multi-Agent Systems*, vol. 13, no. 2, pp. 119–154, 2006.

[92] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust," in *Proceedings of the 13th international conference on World Wide Web*, pp. 403–412, ACM, 2004.

[93] C. Hazard and M. Singh, "An architectural approach to combining trust and reputation," in *The Thirteenth International Workshop on Trust in Agent Societies TRUST-2010*, p. 83, 2010.

[94] L. Hurwicz, "On the existence of allocation systems whose manipulative Nash equilibria are Pareto optimal." Unpublished, 1975.

[95] J. Green and J. Laffont, "Characterization of satisfactory mechanisms for the revelation of preferences for public goods," *Econometrica*, vol. 45, no. 2,

pp. 427–438, 1977.

[96] J. B. McDonald and Y. J. Xu, "A generalization of the beta distribution with applications," *Journal of Econometrics, Elsevier*, vol. 66, no. 1, pp. 133–152, 1995.

[97] R. Bhattacharjee and A. Goel, "Avoiding ballot stuffing in ebay-like reputation systems," in *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, pp. 133–137, ACM, 2005.

[98] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," in *Proceedings of the 2nd ACM conference on Electronic commerce*, p. 157, ACM, 2000.

[99] A. Cheng and E. Friedman, "Sybilproof reputation mechanisms," in *Proceedings of the 2005 ACM SIGCOMM workshop on Economics of peer-to-peer systems*, pp. 128–132, ACM, 2005.

[100] M. Srivatsa, L. Xiong, and L. Liu, "Trustguard: countering vulnerabilities in reputation management for decentralized overlay networks," in *Proceedings of the 14th international conference on World Wide Web*, pp. 422–431, ACM, 2005.

[101] A. Jøsang, "Robustness of trust and reputation systems: Does it matter?," *Trust Management VI*, pp. 253–262, 2012.

[102] B. Levine, C. Shields, and N. Margolin, "A survey of solutions to the sybil attack," *University of Massachusetts Amherst, Amherst, MA*, 2006.

[103] R. Ssekibuule, "Security in Agent-Mediated Negotiation Frameworks," *In Proceedings of the Twentieth European Meeting on Cybernetics and Systems Research*, 2010.

[104] R. Ssekibuule, J. A. Quinn, and K. Leyton-Brown, "A Mobile Market for Agricultural Trade in Uganda," *Proceedings of the 4th Annual Symposium on Computing for Development*, 2013.

[105] R. Ssekibuule, "Mobile-Agent Security Against Malicious Platforms," *In Cybernetics and Systems An International Journal*, vol. 41, no. 07, 2010.

[106] R. Ssekibuule and J. G. Quenum, " Security Analysis of an Agent-Mediated BookTrading Application," *In proceedings of the 5th Annual International Conference on Computing and ICT Research*, 2009.

[107] R. Ssekibuule, "Secure Publish-Subscribe Mediated Virtual Organizations," *In Ninth Information Security South Africa*, 2010.

[108] R. Ssekibuule, "Shilling Countermeasures in Autonomic E-Markets," *In proceedings of the 6th Annual International Conference on Computing and ICT Research*, 2010.

[109] A. Király and J. Abonyi, "Redesign of the supply of mobile mechanics based on a novel genetic optimization algorithm using google maps api," *Engineering Applications of Artificial Intelligence*, vol. 38, pp. 122–130, 2015.

[110] M. Haklay and P. Weber, "Openstreetmap: User-generated street maps," *IEEE Pervasive Computing*, vol. 7, no. 4, pp. 12–18, 2008.

[111] B. A. Johnson and K. Iizuka, "Integrating openstreetmap crowdsourced data and landsat time-series imagery for rapid land use/land cover (lulc) mapping: Case study of the laguna de bay area of the philippines," *Applied Geography*, vol. 67, pp. 140–149, 2016.

[112] N. Suri, J. Bradshaw, M. Breedy, P. Groth, G. Hill, R. Jeffers, T. Mitrovich, B. Pouliot, and D. Smith, "NOMADS: toward a strong and safe mobile agent system," *Proceedings of the fourth international conference on Autonomous agents*, pp. 163–164, 2000.

[113] Q. Mahmoud and L. Yu, "Havana: a mobile agent platform for seamless integration with the existing Web infrastructure," *Electrical and Computer Engineering, 2004. Canadian Conference on*, vol. 3, 2004.

[114] F. Bellifemine, G. Caire, and D. Greenwood, *Developing Multi-agent Systems with JADE*. Springer, 2007.

[115] D. Lange, M. Oshima, G. Kargoth, and K. Kosaka, "Aglets: Programming Mobile Agents in Java," *Lecture Notes in Computer Science*, pp. 253–266, 1997.

[116] X. Li, A. Zhang, J. Sun, and Z. Yin, "The Research of Mobile Agent Security," *Lecture Notes in Computer Science*, pp. 187–190, 2004.

[117] W. Farmer, J. Guttman, and V. Swarup, "Security for Mobile Agents: Issues and Requirements," *Proceedings of the 19th National Information Systems Security Conference*, vol. 2, pp. 591–597, 1996.

[118] W. Jansen, "Countermeasures for mobile agent security," *Computer Communications*, vol. 23, no. 17, pp. 1667–1676, 2000.

[119] MySQL, AB, "MySQL Database Server," *Internet WWW page, at URL: http://www. mysql. com (last accessed 5/21/2011)*.

[120] M. Howard and S. Lipner, *The Security Development Lifecycle*, ch. Risk Analysis, pp. 114–115. Microsoft Press Redmond, WA, USA, 2006.

[121] D. de Groot and F. Brazier, "Identity Management in Agent Systems," *Proceedings of the First International Workshop on Privacy and Security in Agent-based Collaborative Environments (PSACE)*, pp. 23–34, 2006.

[122] "Kerberos: An Authentication Service for Open Network Systems," *Proc. Winter USENIX Conference*, 1988.

[123] B. Kaliski and M. Robshaw, "Message authentication with MD5," *CryptoBytes (RSA Labs Technical Newsletter)*, vol. 1, no. 1, 1995.

[124] F. Bellifemine, A. Poggi, and G. Rimassa, "JADE–A FIPA-compliant agent framework," *Proceedings of PAAM*, vol. 99, pp. 97–108, 1999.