STRATEGYPROOF TRUST MANAGEMENT IN WIRELESS AD HOC NETWORK

huiping Sun, Junde Song
Beijing University of Posts and Telecommunications, Beijing, P.R.China
huipingsun@263.net, jdsong@bupt.edu.cn

Abstract

Trust management is basic component for wireless ad hoc network. Some existing trust management mainly aims to internet application and generally depends on centralized trusted third party. Inherent characteristic of wireless ad hoc network mounts more challenge to design and deploy trust management in wireless ad hoc network.

This paper proposes strategyproof trust management system fitting to wireless ad hoc network. This system is incentive compatible in which nodes can honestly report trust evident and truthfully compute and broadcast trust value of themselves and other nodes.

Keywords: *Trust management; Strategyproof; Wireless ad hoc network.*

1. INTRODUCTION

1.1 Background

Wireless Ad Hoc network [1], [2] is a new wireless network lacking a fixed infrastructure. This network is easy to deploy and owns good anti-destroy because its information transmission depends on cooperation of nodes. There have large numbers of applications including military and rescue mission, business conference, visual classroom, personal area network, ubiquitous computing and wireless sensor network.

Trust management [3], [5], [6], [10] manages and controls trust relationship among entities including generation, discovery, computation and distribution of trust information. It has been merged into some basic operations in wireless ad hoc network such as resource allocation, system management, trust routing, group communication and so on. Owing to the inherent characteristic of wireless ad hoc network such as dynamic topology, node mobility, limited resource and rational user, existing trust management system usually encounters some problems to apply into wireless ad hoc network.

1.2 Contribution

In this paper, we present a framework of strategyproof trust management based on game theory and distributed algorithmic mechanism design (DAMD) [9]. This trust management system is incentive compatible in which nodes can honestly report trust evident and truthfully compute and broadcast trust value of themselves and other nodes.

By introducing cooperative compensate function which rewards cooperation and punishes selfish and malicious behavior, honest participation in trust management becomes dominant strategy of node. This mechanism may greatly reduce overhead and cost of trust management since nodes are truthfully collecting, aggregating, computing and distributing trust information.

1.3 Roadmap

The rest of the paper is organized as follows. Section 2 describes trust definition and characteristic, and analyzes the challenges of trust management in wireless ad hoc network, then lists some guidelines, at last describes some advantages by importing strategyproof to trust management; Section 3 proposes strategyproof trust management mechanism based on game theory and distributed algorithm mechanism design. Future work and conclusion are presented in Section 4 and Section 5.

2. FRAMEWORK

2.1 Trust

It is very difficult to give an explicit definition to trust. In this paper, we use Gambetta's definition of trust [4]:

"Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another or group of agents will perform a

CCECE 2004- CCGEI 2004, Niagara Falls, May/mai 2004
0-7803-8253-6/04/$17.00 ©2004 IEEE

particular action, both before he can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a content in which it affects his own action".

This definition and some related studies [3], [5] indicate that trust is subject, non-symmetry, non-transitive and context-dependent. As a tool describing trust relationship, trust management should offer some means to embody above-mentioned trust properties. Main trust management system of conventional network can't entirely involve all trust properties.

2.2 Challenges

- There is no central authority or trusted third party in wireless ad hoc network to take charge of collecting, maintaining and storing related trust data. It increases difficulty of monitoring trust evident and managing trust relationship.
- Node may interact with many nodes due to node mobility and dynamic topology. Complex and variable trust relationship among nodes introduces challenges how to effectively deal with these relationships.
- Limited resources of node require trust management to accord with processor capability, memory and limited energy of node.
- For increasing itself trust value or decreasing trustworthiness of other nodes, rational node in wireless ad hoc network has strong incentive to misrepresent trust evident or falsely implement trust computing because more trustworthiness can receive more benefit in future interaction.
- In self-organized environment of wireless ad hoc network, everyone node only knows partial trust data about itself and other nodes. It learns and estimates trustworthiness of unfamiliar node by trust recommendation or computation coming from other nodes.
- Some schemes utilize recommending, referring social network analyzing, bayesian learning or other method to receive trust and reputation information. This process of trust learning and estimating requires network has long-term interaction and high population.

2.3 Guidelines

- System must provide enough incentive to stimulate rational and self-interested user to take part of trust management because all of functions in wireless ad hoc network are depended on cooperation among nodes.
- System should represent all necessary trust properties. For example, trust is subject and context-dependent concept so trust management should compute trust value according actual environment.

2.4 Strategyproof

Strategyproof [7], [8], [9] is a compelling concept coming from mechanism design (MD) [11] which takes participant as a rational node following game theory. Self-interested node can maximize her own utility through straightforward truth-revelation about requirements and capabilities, whatever the strategies and behaviors of other parties. A common example of strategyproof mechanisms is the second-price auction.

If we can construct a strategyproof mechanism in trust management system, each node honestly reports its trustworthiness will become a dominant strategy whatever any other node reports. It will greatly reduce overhead and cost of trust management since nodes are truthfully collecting, aggregating, computing and distributing trust information.

3. SYSTEM

3.1 Model

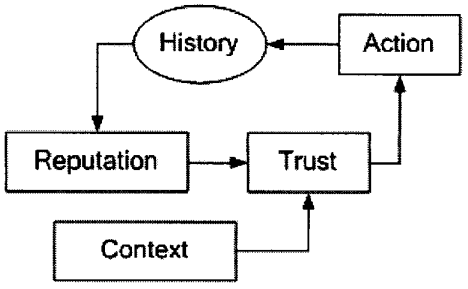

Figure 1. Trust Management Model

Figure 1 shows system model on trust and reputation. First, trust is subject and context-dependent. The computation of trustworthiness depends on not only reputation value of node but also context of node such as load, location of node, security evaluation of environment, time and so on. Second, the action history is one data source of reputation computation and the other is recommended by other node. Third, based on reputation and a special context, node can calculate to its trustworthiness fitting for this environment.

Reputation value and trustworthiness is privacy information of node. Node must announce its trustworthiness before interfacing with other nodes. This

declaration may is untruthful because node has incentive to magnify and reduce actual trustworthiness for maximizing its payoff.

3.2 Assumption

- Node can not collude with other nodes;
- Node is greedy in reputation increasing;
- Trustworthiness of node is a probability;
- Utility function u_i is quasilinear;
- Using reputation acts as node's welfare;

3.3 Concept

This paper envisions a wireless ad hoc network with n nodes $N = \{1, 2, ..., n\}$. There have some parameter as following:

- t_i : trustworthiness of node i;
- r_i : reputation value of node i;
- u_i : utility function of node i;
- p_i : payment function of node i;
- $\tilde{t}_i$: declaring trustworthiness of node i;
- O : a output function;
- T : trustworthiness space;
- R : reputation value space
- $\tilde{T}$: declaring trustworthiness space;
- X : system decision space

There have some definitions and formula according to mechanism design theory as following:

- $O : \tilde{T}^n \to \mathrm{X}$
- $p_i : \tilde{T}^n \to \mathbb{R}$
- $\tilde{T} = \{\tilde{t}_1, \tilde{t}_2, ..., \tilde{t}_n\}$
- $t_{-i} = \{t_1, ..., t_{i-1}, ...t_{i+1}, ...t_n\}$
- $u_i(\tilde{T}) = t_i(O(\tilde{T})) + p_i(\tilde{T})$

A mechanism is strategyproof in this system if

$$u_i(T) \geq u_i(t_{-i}, x_i), \quad for\ all\ x_i$$

3.4 VCG Mechanism

Vickrey-Clarke-Groves (VCG) [8] is a distinguished mechanism which is both strategyproof and efficient. The initial ideas of VCG come from second-price sealed auction. Now, VCG is headwaters of many strategyproof algorithms and have plentiful applications in trade, auction, network formation and so on.

There exists a VCG mechanism in aforementioned example of trust management, choice and payment rule is as follows.

$$O^*(\tilde{t}_i) = \arg\max_{o \in O} \sum_{j \in N} v_i(o, \tilde{t}_j)$$

$$p_i(\tilde{t}_i) = \sum_{j \in N \setminus i} u_j(O^*_{-i}, \tilde{t}_j) - \sum_{j \in N \setminus i} u_j(O^*, \tilde{t}_j)$$

3.5 Payment function

The function of payment function is to add or reduce reputation value of some node. Whether a mechanism is strategyproof or not depends on choose of payment function. There have two class methods to carry out this task.

- Auction-based

The theory foundation of this method is VCG or some similar auction theory. It constitutes some bidding or auction context in application environment of trust management.

- Check-based

Based on support of centralized infrastructure or some cooperative broker, node can receive some useful information. Node can adjust its strategy in order to influence compensate function.

4. FUTURE WORK

For a fresh user who does not have much experience, we are trying to refine this system through strategyproof trust management system is somewhat complex. There have four immediate works will be done:

- This paper only gives a framework of strategyproof trust management system, some parts need to deal with in the future.
- Payment function in this paper only has a coarse idea. Finding general construction method is needed.
- There have many basic functions needed to receive support of trust management system, applying proposed system in this paper into these functions is a good topic.
- This paper assumes that node can not collude with other nodes. This assumption is too ideal for wireless ad hoc network. How to construct group-strategyproof trust management is one of future work.

5. CONCLUSIONS

This paper first analyzes shortcomings of existing trust management system, surveys some challenges that we will face to deploy trust management into wireless ad hoc network, and presents some guidelines.

In this paper we propose a strategyproof reputation management system by inject strategyproof into trust management system. Relying on payment function to reward honesty and punish cheat, Nodes has to truthfully reveal their trustworthiness in interface with other nodes. It makes this system has low overhead and good efficiency.

References

[1] S. Giordano, "Mobile Ad-Hoc Networks", Book chapter in Handbook of Wireless Networks and Mobile Computing. John Wiley & Sons. Feb 2002.

[2] Levente Buttyan and Jean-Pierre Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks", ACM Mobile Computing and Communications Review. Vol.6, No.4, October 2002.

[3] Birk, A. "Learning to Trust In R. Falcone, M. Singh and Y.-H. Tan (Eds.): Trust in Cybersocieties", LNAI 2246, pp. 27-54, 2001 © Springer-Verlag Berlin Heidelberg 2001

[4] Gambetta, Diego, "Can We Trust Trust? In Gambetta, Diego(ed.) Trust: Making and Breaking Cooperative Relations", Department of Sociology, University of Oxford, charpter 13, pp.213-237, 2000.

[5] Alfarez Abdul-Rahman,Stephen Hailes, "Using Recommendations for Managing Trust in Distributed Systems", In Proceedings IEEE Malaysia International Conference on Communication'97 (MICC'97), Kuala Lumpur, Malaysia. November 1997.

[6] Resnick, P, Zeckhauser, R, Friedman, E., Kuwabara, K, "Reputation Systems", Communications of the ACM, 43(12):45-48, 2000.

[7] J. Shneidman and D. C. Parkes, "Rationality and self-interest in peer to peer networks", In 2nd Int. Workshop onPeer-to-Peer Systems (IPTPS'03), 2003.

[8] D. C. Parkes, "Iterative Combinatorial Auctions: Achieving Economic and Computational Efficiency", PhD thesis, Department of Computer and Information Science, University of Pennsylvania, May 2001.

[9] J. Feigenbaum and S. Shenker, "Distributed Algorithmic Mechanism Design: Recent Results and Future Directions", In Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, pages 1–13, 2002.

[10] B. Yu and M. Singh, "An Evidential Model of Distributed Reputation Management", In Proceedings of the AAMAS, Bologna, Italy, 2002.

[11] N. Nisan and A. Ronen, "Algorithmic mechanism design", Games and Economic Behavior, 35:166–196, 2001.