2010 Fifth IEEE International Symposium on Service Oriented System Engineering

MobiCloud: Building Secure Cloud Framework for Mobile Computing And Communication

Dijiang Huang
Computer Science Engineering, ASU
Tempe, USA

Xinwen Zhang
Samsung R&D Center
San Jose, USA

Myong Kang, Jim Luo
Naval Research Lab
Washington DC, USA

***Abstract*—Cloud services can greatly enhance the computing capability of mobile devices. Mobile users can rely on the cloud to perform computationally intensive operations such as searching, data mining, and multimedia processing. In this paper, we propose a new mobile cloud framework called *MobiCloud*. In addition to providing traditional computation services, MobiCloud also enhances the operation of the ad hoc network itself by treating mobile devices as service nodes. The MobiCloud framework will enhance communication by addressing trust management, secure routing, and risk management issues in the network. A new class of applications can be developed using the enhanced processing power and connectivity provided by MobiCloud. Open research issues for MobiCloud are also discussed to outline future research directions.**

***Keywords*-Mobile Ad Hoc Network, Cloud Computing, Context-awareness, Security.**

I. Introduction

The use of mobile devices to establish ad-hoc communication systems is a viable solution that provides global connectivity to support a broad range of applications. With the development of wireless access technologies such as 3/4G, LTE, and WiMax, mobile devices can gain access to the network core over longer distances and larger bandwidths. This allows for very effective communication between mobile devices and the cloud infrastructure. A new service architecture is necessary to address the requirements of users in their unique operational environment and create new mobile applications. In general, mobile users can benefit greatly from cloud services for computationally intensive information processing and collection such as information search, data processing, data mining, network status monitoring, field sensing, etc. However, existing mobile cloud service model operates mostly one-directional. For example, consumer electronics (CE) devices can use the cloud as a computing and information resource. Operations can be outsourced to the cloud, but the cloud has little control over the CE devices.

The objective of our research is to use a systematic approach to investigate both cloud computing and mobile ad hoc networks (MANETs) technologies in order to understand the capability of cloud computing for securing MANET applications. This research article is presented as a position paper to highlight research directions and possible solutions for enhancing secure mobile computing using cloud computing. We present a new MANET communication framework named MobiCloud that will fundamentally change the research and development of secure MANET technologies. Furthermore, we will identify a number of open research issues that will provide guidance for the cloud computing and MANET research communities to developing new solutions for secure mobile computing.

Building a trustworthy MANET communication system is one of the most challenging research issues of mobile computing. This is caused mainly by two inter-related research issues: (1) the security of existing MANET infrastructure lacks inter-operability support in a heterogeneous communication environment. Communication devices belonging to different administrative domains with different communication and computation capabilities make protocol design extremely difficult. This issue is usually caused by the uncertainty in the security setup of communications peers during trust establishment. For example, mobile entities may use different identity space, cryptographic parameters, and reside in different administrative domains. (2) MANET mobility has a significant impact on the security and communication performance relating to location tracking, communication privacy, reliability and survivability. Uncertainty introduced by mobility produces unpredictable inter-meeting duration, transmission rates, and locations. Therefore, the MANET operations require a comprehensive approach focusing on risk assessment with respect to security and communication requirements.

MobiCloud transforms traditional MANETs into a new service-oriented communication architecture. MobiCloud transforms each mobile node from a traditional strictly layer-structured communication node into a service node (SN). Each SN can be used as a service provider or a service broker according its capability, e.g., available computation and communication capabilities to support a particular service. This approach takes maximum advantage of each mobile node in the system by utilizing cloud computing technologies. To reduce the uncertainty caused by mobility, we incorporate every SN into the MobiCloud as a virtualized component. Each SN is mirrored to one or more Extended Semi-Shadow Images (ESSIs) in the cloud in order to address the communication and computation deficiencies of mobile device. We note that ESSI can be differentiated from a virtual image" in that an ESSI can be an exact clone, a partial clone, or an image containing extended functions of the physical device. In addition, the ESSIs create a virtualized MANET routing and communication layer that can assist the physical mobile nodes

978-0-7695-4081-8/10 $26.00 © 2010 IEEE
DOI 10.1109/SOSE.2010.20

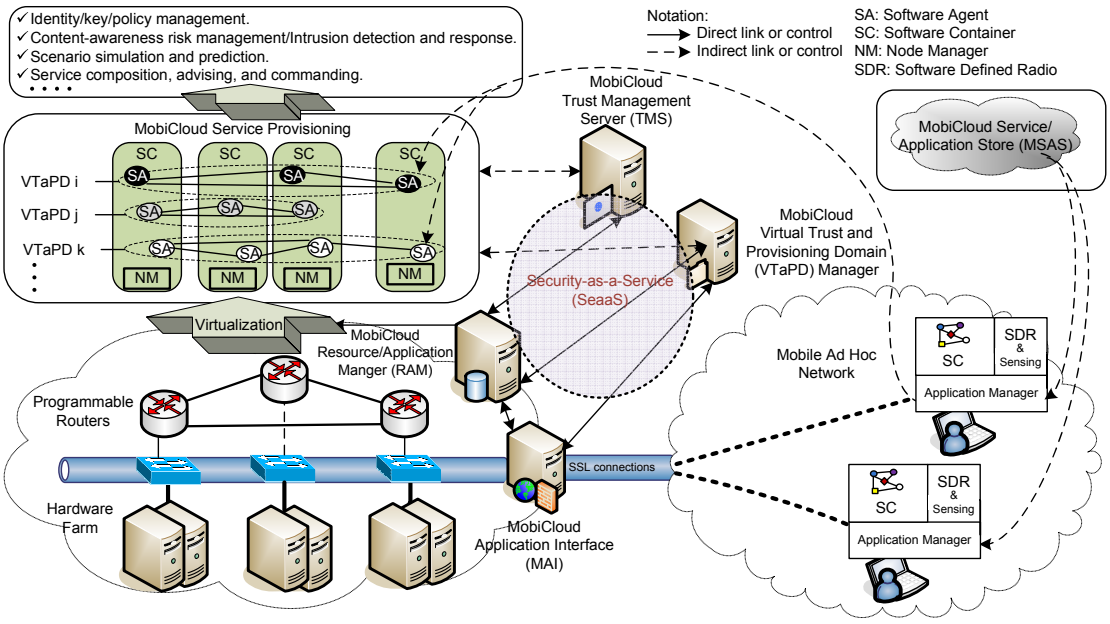

Fig. 1. Reference Model of MobiCloud.

and maximize availability of pervasive computing services for each mobile user. The main contributions of this research paper are summarized as follows:

- MobiCloud supports the MANET functions of information dissemination, routing, localization, and trust management.
- MobiCloud adopts cloud computing technology to create a virtualized environment for MANET operations in multiple service provisioning domains according to the criticality of MANET services and corresponding security requirements.
- MobiCloud provides a fundamental trust model including identity management, key management, and security data access policy enforcement that can be used to develop future mobile applications.
- MobiCloud supports the MANET operations through research on context-aware risk assessment using communication and performance metrics of each mobile node under corresponding security requirements. This will allow us to use the MobiCloud to inspect various performance and security issues of MANET and generate useful data.

The rest of this paper is arranged as follows: In Section II, we present recent research in both cloud computing and secure MANET communication. The detailed description of MobiCloud is presented in Section III. In Section IV, we present new applications that can be supported by using MobiCloud. Finally, we summarize the proposed solution and present open research issues in Section V.

II. Related Work

In this section, we presented related work in two areas: security in cloud computing and secure MANET communication using cloud computing.

Cloud computing is a new business model focusing on resource-on-demand, pay-as-you-go, and utility-computing [1]. Cloud computing can be broadly classified as infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Critical research issues for cloud computing such as computation offloading, remote execution, and dynamic composition have been extensively discussed in previous literature. Several approached have been proposed on enhancing security of Clouds themselves, such as infrastructure security [2] based on TCG/TPM [3], secure outsourcing [4], [5], [6], [7], cloud web security [8], [9], resource management and isolation [10], [11], and privacy [12], [13].

Recent research have been focused on cloud computing for mobile devices [14], [15], [14], [16]. Cloud computing for mobile devices has a major benefit in that it enables running applications between resource-constrained devices and Internet-based Clouds. Moreover, resource-constrained devices can outsource computation/communication/resource intensive operations to the cloud. CloneCloud [17] focuses on execution augmentation with less consideration on user preference or device status. Samsung has proposed the concept of elastic applications which can offload components of applications from mobile devices to cloud [18]. Oberheide et al. [19] present a framework that outsources the anti-virus services from mobile devices to a cloud. Goayl and Carter propose a secure cyber foraging mechanism for resource-constrained devices [20]. Existing mobile cloud solutions are limited and

focuses solely on enhancing the capability mobile device on an individual basis.

III. MobiCloud Architecture

In this Section, we first describe the MobiCloud architecture (shown in Figure 1) and its support for security service provisioning, resource and security isolation, and the integration of processing and operations of cloud and MANETs. We then describe several services that can help both cloud and MANET to achieve the proposed system-level functionalities, such as identity management, key management, policy enforcement, and context-aware routing and risk assessment.

A. MobiCloud Security Services Architecture

1) MobiCloud Architecture: Figure 1 shows the conceptual infrastructure for MobiCloud. Similar to existing cloud-based computation and storage outsourcing [18], a mobile node can leverage hardware farms on cloud to augment its computing capabilities. Beyond this, we introduce a new type of service named "virtual trusted and provisioning domain (VTaPD)" to isolate information flows belonging to different security domains using programmable router technologies [21]. Moreover, we provide fine-grained trust management and feedback/command capability to mobile users. In summary, MobiCloud is designed to provide the following cloud services for MANETs:

- Serve as an arbitrator for identity, key, and secure data access policy management.
- Provide security isolations to protect mobile users' information.
- Monitor MANET status for risk assessments, intrusion detection and response.
- Simulate scenarios and predict future MANET situations for decision making.
- Provide service composition and applications for mobile devices.

Now, we describe the functionality and properties of each component of Figure 1. MobiCloud uses Software Agents (SAs) (i.e., application components) to link the cloud services and mobile devices. The same SA can run on both the mobile device and the cloud platforms correspondingly. Each device can have multiple SAs for different cloud services or MANETS, which are managed by application manager of the device. Each device also provides sensing data about the device itself (such as processor type, utilization, battery state, and location with GPS support), and about the neighboring mobile nodes (such as neighbor's identity or addresses, link quality, neighboring durations, etc.), which are managed by the sensor manager.

On the cloud side, the MobiCloud Application Interface (MAI) exports services that can be consumed by to mobile devices. In addition, the MAI also provide interfaces to VTaPD manager and Resource and Application Manager (RAM). Middle-ware based solutions are required when the cloud components do not use web-based interfaces. Several unique cloud components and constructions are proposed for MobiCloud. We introduce programmable routers that can be used to create multiple VTaPDs. VTaPDs are created mainly for isolating information flow and access control by creating multiple virtual domains. There are two main reasons for multiple virtual domains: (1) security, a user's device may run multiple applications at different security domains, e.g., its simultaneous communication with two individuals with from administrative domains; and (2) context-awareness, it may be necessary to separate services for different local and network settings. For example, MobiCloud can simulate the operations of the MANETs using different system parameters or routes selection algorithms to compare different approaches for utilizing cloud computing and communication resources. This approach provides a comprehensive overview of MANET operations and provides information to mobile devices and system managers for decision making.

In each VTaPD, one or more SAs are used for every ESSI. A Node Manager (NM) is responsible for managing the loading and unloading of SAs in the ESSI. The ESSI also provides additional capabilities beyond the functions of a mobile device. For example, the cloud will be able to run services that are not available in MANETs, such as search, data mining, media processing, trust pre-establishment (e.g., credential exchange and establishing security keys in advance), etc. The MobiCloud Resource and Application Manager (RAM) constructs VTaPDs when it is directed by MobiCloud VTaPD manager and MobiCloud Trust Manager Server (TMS). They form the core for providing Security-as-a-Service (SeaaS). With SeaaS, MobiCloud can offer security service composition capability according to requests from mobile applications. In our SeaaS service model, the VTaPD manager plays the central role since it collects context-awareness information from the MANET (such as device sensing values, location, and neighboring device status) and used it for intrusion detection and risk management. The MobiCloud TMS is the Trust Authority (TA) for MobiCloud. It handles the attribute-based key distribution and revocation. It provides identity search and federation services for mobile devices belonging to multiple administrative domains. It also performs policy checking and enforcement functions to provide a unified trust management system for MobiCloud.

Finally, the MobiCloud Service and Application Store (MSAS) serves as the repository for SAs and applications. When service composition is needed, the MSAS will install the required SAs or applications through the MAI. For example, when a mobile device needs to talk to another device using different frequency bands, the Software Defined Radio (SDR) needs to install a new driver and the node needs another authentication module. In this scenario, the SAs for the new drivers and authentication module will be installed. This operation needs collaborations between TMS and MSAS.

2) Secure Isolation through VTaPDs: VTaPDs are established to provide data access control and information protection. We must note that the framework may not need/imply the division of the administrative domain into VTaPDs. In the following subsection, we will address the cloud resource

isolation and security isolation.

Resource isolation: The actual administrative work is handled by the MobiCloud VTaPD manager. Every node that belongs to a particular VTaPD will have the complete routing information for VTaPD in which it resides, but not others. Each node can reside a different physical system. Each node would have to support our communications framework which includes secure group communication to sending data to all the ESSIs in the same VTaPD. The bandwidth for a communication link can be divided by using different encryption/decryption/authentication keys. An advantage of the MobiCloud framework that provides network virtualization through multiple VTaPDs is that it facilitates prioritization of critical/emergency services in a network. For example, using the proposed virtualization approach, prioritized and normal service classes can be defined using different VTaPDs. They can share the same physical MANET but prioritized based on the VTaPD. MANET operations and communications can be migrated into the cloud when peer-to-peer communication is under stress either from insufficient bandwidth or attacks.

Data access control: In addition to the isolation provided by VTaPD service domain, MobiCloud also needs to integrate data access control and information isolation using a cryptography based approach. Besides the traditional security concerns (i.e., authentication, authorization, audit etc.), additional security risks are introduced by mobile users who share the same application instance and resources. In cloud related literature, this referred to as multi-tenant environments. Each mobile user's ESSI can be considered as his/her tenancy in the MobiCloud. In the multi-tenant environment, data access control is one of the most critical security concerns that need to be addressed. Data isolation mechanisms prevent users from accessing resources belonging to other tenants. There are generally two kinds of access control isolation patterns: implicit filter and explicit permission. Chong et al. [22] introduced how to apply these two patterns into a multi-tenant data model. We further generalize the two patterns to provide access control for other resources:

- *Implicit Filter Based Access Control Isolation*: In this pattern, when one tenant requests to access shared resources, a common platform level account (i.e., the ESSI identity with corresponding SA and cloud resource requests) is delegated to handle this request. The delegated account is shared by all tenants and has the privileges to access resources of all tenants. However, the key of this mechanism is to implicitly compose a tenant-oriented filter that will be used to prevent one user from tapping into resources of other tenants. This can be achieved by using a cryptography-based solution, i.e., group key management based solutions to secure information flow through different VTaPDs that share the same physical system.
- *Explicit Permission Based Access Control Isolation*: In this pattern, access privileges for the resources have been explicitly pre-assigned to the corresponding tenant accounts by using the Access Control List (ACL) mechanism. Therefore, there is no need to leverage an additional common delegated account across tenants.

B. MobiCloud Trust Management

Several interrelated components of trust management in MobiCloud will be addressed including identity management, key management, efficient data access control, and security context-aware-based risk assessment. Moreover, we will present an approach to incorporate cloud computing techniques to address several research issues considered very difficult problems for MANETs.

1) MobiCloud Identity Management: The user-centric identity management, which is also frequently referred to as identity 2.0, allows an individual to have multiple identifiers. For example, the identifier carried on a national ID card becomes just one of many of an individual's identifiers, which can also include passport ID, club card ID, military ID, email ID, unique MAC/IP address, etc. There are many research problems may in this area. How to provide convenient secure single sign-on to multiple distinct entities? How to give individuals fine-grained control for the sharing specific personal identities between entities when it is to their advantage to do so? How do we know what identity information to share when two users meet? To address these questions, we propose a novel Attribute-Based Identity Management (ABIDM).

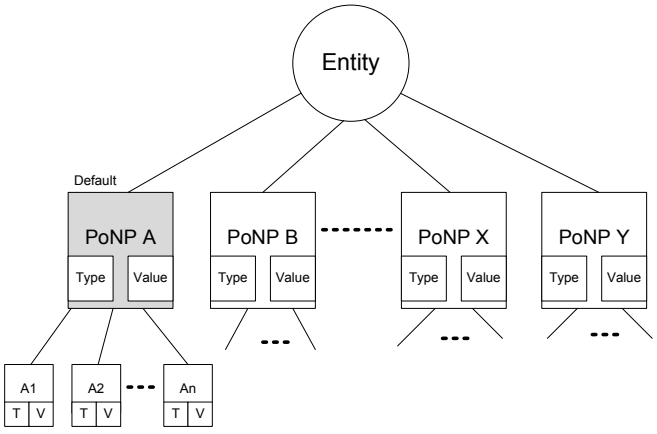

Fig. 2. Identity representation scheme.

The basic identity representation of ABIDM is shown in Figure 2. Using ABIDM, we first need to define the point of network presence (PoNP). A mobile node's relationship can be thought of as lines radiating from the PoNP to the various counterparties. Each line is distinct and tagged with the attribute used by a particular counterparty. In particular, we define a default PoNP (i.e., native PoNP) for each individual. The default PoNP has to be linked by a unique native ID. The uniqueness of the native ID is not difficult to achieve. Indeed, any user can have a unique native ID by simply hashing any one of his/her unique identifiers, such as military ID, SSN, etc. It is not necessary to use identifiers from the same administrative domain. Each PoNP has two properties:

type and value. Each PoNP is associates with one or multiple attributes (A1...An), and each attribute has type and value properties.

The major benefit of using this identity representation is the standardization" of identity management. In practice, the numbers of PoNPs for every mobile node should not be many. They can be assigned to mobile users as predefined attributes that that do not changed frequently. We call these attributes as static attributes. To differentiate PoNPs, we will be able to narrow down the numbers of attributes that can be potentially used for later secure communications.

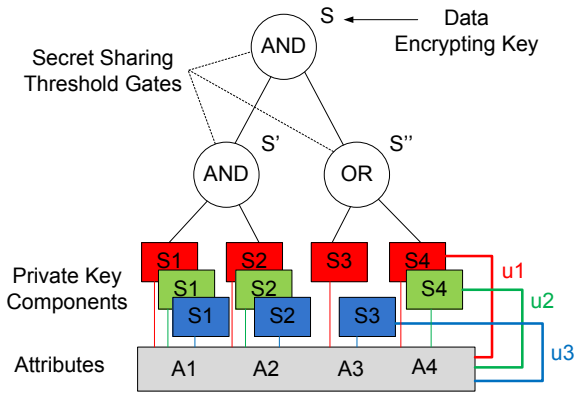

Fig. 3. Attribute-based Encryption.

2) Efficient Key Management for Secure and Private Data Access Control: In Figure 3, we present an example to illustrate using ABE [23] for data encryption and decryption. In this example, attributes $A1 - A4$ are arranged as leaf nodes of the attribute tree. Each attribute can have multiple secret components for different users. We must note that users can share an attribute; however the corresponding private key components for that attribute are different. This is represented by different colors of the keys. Thus, $u1$ has private key components $\{red : S1, S2, S3, S4\}$, $u2$ has private key components $\{green : S1, S2, S4\}$, and $u3$ has private key components $\{blue : S1, S2, S3\}$. The internal nodes of the attribute tree are logical gates, such as AND, OR. They are implemented using threshold secret sharing scheme [24]. The secret S can be derived from S' and S'' using the secret sharing scheme. At the bottom level the encryption is performed using a construction similar to identity-based encryption (IBE) [25]. During encryption, in order to satisfy the AND gate, the decrypter must have all the secrets under it to reconstruct the higher level secret; to satisfy the OR gate, the decrypter is only required to have one of the secrets. The encryption algorithm of ABE is performed in a top-down manner by constructing the ciphertext at the bottom level of the attribute tree. The decryption algorithm of ABE is performed in a bottom-up manner using the users' pre-distributed secrets to reconstruct higher level secrets until they reach the root. In this presented example, based on the pre-distributed secrets, $u1 - u3$ can decrypt the secret S and thus they can access the data encrypted by using the DEK S.

Existing key management solutions usually consider the key management and Identity Management (IDM) as different issues. We use a novel key management solution, i.e., ABKM, to integrate key management and IDM. In ABKM, we can simply consider all the attributes belong to an entity as its public key. Each attribute can be considered as a public key component, and each of the attributes is also paired with a private key component. The private key, which is in turn is formed by multiple private key components, is distributed from a TA. We must note that ABKM is basically an extended version of identity-based cryptography, in which the identity can be considered multiple descriptive attributes and the attributes can be used to represent descriptive policies through logical operators such as "AND" and "OR". Compared to traditional PKI based key management solutions where a user's private key is only known to the public owner, using ABKM, the TA generates private key components for each user according to his/her public attributes. This approach delivers a major benefit in that the private key can be generated for descriptive terms or statements instead of using a large random number (e.g., RSA). The descriptive terms can be used to specify data access control policies, which is very efficient in terms of security policy management. For example, traditional data access control approaches usually use a key exchange protocol to distribute the Data Encrypting Key (DEK) to a user to decrypt the ciphertext. However, using ABKM, the key exchange protocol is not needed. The sender can just simply select a set of attributes according to required security policies to generate the ciphertext. This property is very useful in delay tolerant MANETs since a source usually does not need to talk with the destination before sending him/her the data. Moreover, the data access can be very flexible, where the data sender does not need to know the identities of receivers. In fact, this approach is very effective for secure group communication, where a group of receivers may satisfy the specified data access policies. Furthermore, a policy tree can be used for secure group communication since attributes can be used to specify a group of users, which make the ABKM approach appealing in large-scale communication systems.

3) Context-aware Risk Management in MobiCloud: Risk management calls for the identification, assessment, and prioritization of risks followed by a coordinated and economical application of available resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities [26]. The methods, definitions, and goals vary widely in MANETs according to whether the risk management method is in the context of the mission supporting functions, operations, or security. Here, we focus on two important components of risk management: context-aware routing and intrusion detection/response.

Context-aware Routing: Context awareness is a concept with a broad range of meaning. Literally, it means taking into account the context" while making decisions. However, the definition of context varies depending on the applications, the decisions, as the environments. In MANETs, context-awareness usually means to give consideration to the systems

parameters of the devices (e.g., battery level, CPU power), the networking parameters (e.g., bandwidth, delay, connectivity), the content (e.g., the mission specified goals), and the security (e.g., privacy, location, attacks) when using the network. This is because such environments often have highly dynamic characteristics that can significantly affect applications. In order to provide continuous services in such a highly dynamic network, context-aware service migrations are required so that the applications can be adaptive to volatile contexts. For instance, when a node providing a certain service is running out of battery, the framework should be aware of such context change, and migrate the service (and the entire executing contexts) to another available node.

To achieve context-awareness capability, a mobile node needs to collect its local context information (such as device properties, communication parameters, and security) and periodically send them its ESSI. Comprehensive risk assessment can be performed on the MobiCloud since the status of the entire system (such as end-to-end communication delay, reachability to the destination, security status of each mobile node, etc) is available. If the cost (computed through a utility function) of using ad hoc communications is higher than the cost of sending the information through the cloud, the cloud communications is preferred. The utility functions need to be well designed to operate under various situations in which the mission goals of the tactical MANETs and their corresponding context-related measurement metrics can be different.

Using cloud services, the data collection and processing will be handled in a centralized. As a result, the complexity of context-awareness operations will be greatly reduced. Moreover, simulations can be performed on the MobiCloud to evaluate different modes of operation for the MANETs and then provide better recommendations to mobile nodes. This will reduce the uncertainty of mobile system and thus improve the performance of MANET communications. Particularly, positioning, network topology maintenance, and routing functions can be performed by using cloud services. Each node can get this information from the cloud. In this way, the information dissemination among mobile nodes will become one-to-one communication between the physical device and its shadow image in the cloud, instead of one-to-many communications in traditional MANETs. This will greatly reduce the communication and management overhead among mobile nodes. In addition to the context-based routing, MobiCloud also needs to take into account the contents of messages when making the routing decisions. The MANET mission information is usually contained in the transmitted content. For example, the following content can affect the routing decision: (a) the minimum spanning tree from the message sender, (b) the content predicates of neighbors (e.g., the neighbors' role, processing function on the received data, security clearance level, etc.), and (c) how long each neighbor has been apart from the destination.

MobiCloud Risk Management: Many existing MANET security solutions have tried to protect MANETs using preventive approaches. Although preventive approaches can significantly reduce potential attacks, they cannot counter malicious insiders (from mis-configured or node malfunction). Previous work [27], [28] have proposed to counter identified malicious mobile nodes by isolating uncooperative nodes. From the risk management perspective, the major drawback of the isolation approach is that they do not take into account the negative side effects of the isolation. In some cases, countermeasures to intrusions may cause more damage than the actual identified attacks (e.g. by isolating the entire network). To make a comprehensive risk assessment, centralized data collection and processing is more effective. In the cases of malicious nodes partitioning the networks, the distributed approach will suffer a high false negative rate since attackers can manipulate information within different partitions. MobiCloud can identify malicious nodes and make risk assessment with full knowledge of the entire MANET communication system.

IV. New MobiCloud Application Scenarios

Based on the presented MobiCloud framework, we highlight several application scenarios that traditionally are considered to be difficult in MANETs.

Inter-operable scenario: A search team is searching for a lost individual in an area, where they have located equipment that might belong to the missing person. Due to security protection, the search team cannot read the identification stored in the RFID tag affixed to the equipment. Here, they can proxy the communication between the tag and the back end server running in MobiCloud. In this scenario, interoperability is the major problem, which is caused by two separate issues: (1) two wireless devices running two different protocols (or different versions of software), and (2) two wireless devices belonging to two different administrative domains and thus using different security parameters (e.g., cryptographic keys). To address this problem, the search team's wireless devices may not be preprogrammed to read the RFID tag. However, with software defined radios, the search teams can download the necessary software components from the MobiCloud to enable communications. In the meantime, the cloud can also help the search team set up a secret key between the tag and reader. As another example, if the rescue team needs to locate the individual's location based on the signal transmitted from a wireless device that he/she carries, the rescue team may need new services for location tracking. Localization usually requires a synchronized environment to run a triangulation algorithm. The MobiCloud can compose a time synchronization service and software on wireless devices to enable the ad-hoc positioning capability for rescue team members.

Efficient Communication scenario: Communications overhead due to MANET routing contributes a great portion of MANET bandwidth consumption. To demonstrate the routing overhead, in Figure 4, we present a simulation-based study using the group mobility model [29] for two on-demand routing protocols, AODV [30] and DSR [31], where we deploy 60 mobile nodes and each randomly selects its moving velocity between 10m/s and 30m/s. It shows that the routing traffic ratio to overall traffic increases when less data are transmitted

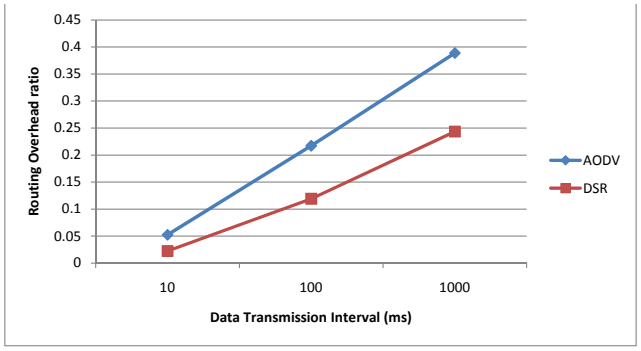

Fig. 4. MANET routing overhead. (a) Routing overhead of overall transmitted data. (b) Number of links broken due to mobility.

(i.e., data packets are sent for every 1 second). This study demonstrates that overall ratio of routing overhead can be even greater when the MANET is under stress, e.g., communication speed is reduced due to poor communication channel quality or frequent link changes among mobile nodes. This will make the MANET data communication more congested. With MobiCloud support, mobile nodes do not need to perform path searching and maintenance for routing purposes; instead, each mobile node only needs to monitor the connectivity and channel quality to its neighboring nodes and updates this information to its ESSI in the cloud. The cloud will perform routing and inform the node on how to forward packets.

Security and service isolation scenario: With the development of wireless technology, a smart phone can serve as a personal information gateway. It can communicate with a variety of wireless devices belonging to different administrative domains. Running more applications will increase the threats of malware that can be installed in the smart devices and then jeopardize the critical information processed in the device. Using MobiCloud, we can initiate one or multiple ESSIs running multiple services on different physical computing systems in the cloud for a mobile device. In this way, attackers can be prevented from manipulating caching operations [32] to steal users' private information in the cloud. Moreover, the system complexity of wireless devices is reduced by running simple and trusted software, and hence the chance of being compromised is also reduced. The isolation of services can also help commanders decide on effective methods to operate the MANET. For example, context-aware routing [33], [34] needs to consider the situations of MANET using a set of predefined parameters (such as battery status, communication channel qualities, previous communication and neighboring history of a node, etc.) to determine a packet forwarding strategy. To this end, the cloud can create a virtual routing domain to emulate the routing behaviors of the MANET and then provide suggestions to commanders for decisions.

Delay tolerance communication scenario: Traditional delay tolerance networks consider each mobile device as both a communication device and a storage device. They maintain received information and deliver this information to the intended destination when they are back online. The uncertainty of this communication model is very high due to unpredictable mobility and storage status of neighboring devices. MobiCloud will reduce the uncertainty by functioning as an information repository. Thus, the message originator, forwarder, and receiver know that the MobiCloud is the repository for sending, forwarding, and retrieving information.

Cloud computing has a great potential to bring more application scenarios than the above mentioned ones for mobile computing applications. Based on the presented new MANET infrastructure, we expect more MobiCloud applications can be identified and developed in near future.

V. Discussions and Future Research Directions

In this paper, we presented a new mobile cloud framework for MANETs called MobiCloud'. We presented a comprehensive framework focusing on important and inter-related system components including virtual trust and provisioning domain construction, resource and information flow isolations, trust management (i.e., identity management and attribute-based data access control), context-aware routing, intrusion detection, and context-aware risk management. Apart from system components discussed, there are several research and implementation issues need to be addressed. They are discussed in the following subsections:

Damage Recovery: The mobile devices such as consumer electronics (CEs) can be lost or stolen. Using MobiCloud, the user's information can be recovered through the corresponding ESSI that stores the data and processing status information. The research challenge is how to prevent malicious attackers from using the mobile devices. Intuitively, biometrics based identification techniques on the CE devices such as voice recognition, fingerprints, etc., can be used as a second authentication method to protect the mobile devices. However, biometrics enabled devices will increase the device cost, and protecting the biometrics's information of a mobile user becomes another issue. Thus, the research question is that can we use MobiCloud to protect user's data, even if the mobile devices are lost or compromised?

Fine-grained Resource and Security Isolation: VTaPD provides a coarse level of isolation, which can be established based on available network resource or totally independent services. However, one service may depend on another service, and two services may share partial data. Thus, it is possible that multiple VTaPDs may share some common resources or data. To address this issue, we should take a fine-grained resource and security isolation approach. One possible solution is to develop an efficient secure many-to-many secure group communication system, where any SA can talk to a subgroup of SAs at the same time based on their service and security requirements. Thus, a fine-grained data access control mechanism is required to construct instant and partially joint VTaPDs. We use μVTaPD to represent such a VTaPD, where μ is used to specify the resource, security, and life-span constrains. In other words, a μVTaPD can be considered as

a supporting VTaPD. How to construct and delete a μVTaPD should be investigated.

Real-time performance issue: Operation delay will be a major evaluation metric for designing MobiCloud applications. This is because interactive MANET communication usually imposes stringent real-time requirements. Thus, the MobiCloud services must not introduce long delays. Particularly, MobiCloud service delay needs to be further investigated by considering three types of MobiCloud services: (i) *Monitoring service*: the cloud collects node and MANET status information from mobile devices and predicts appropriate actions to be taken for mobile devices. (ii) *On-demand service*: the cloud serves as a server, e.g., assisting a mobile node to establish trust with another node controlled in different administrative domains. (iii) *Advising service*: the cloud duplicates/emulates the actions of MANETs for post-event analysis.

ACKNOWLEDGEMENT

The research described in this paper was supported by NSF DUE-0942453.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, *et al.*, "Above the clouds: A berkeley view of cloud computing," *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28*, 2009.

[2] N. Santos, K. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," *Proceedings of USENIX HotCloud*, 2009.

[3] "Tcg specification architecture overview." Available at https://www.trustedcomputinggroup.org.

[4] K. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," in *Proceedings of the ACM workshop on Cloud computing security*, 2009.

[5] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in *Proceedings of the ACM workshop on Cloud computing security*, 2009, pp. 55–66.

[6] A. Yun, C. Shi, and Y. Kim, "On protecting integrity and confidentiality of cryptographic file system for outsourced storage," in *Proceedings of the ACM workshop on Cloud computing security*, 2009, pp. 67–76.

[7] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the ACM workshop on Cloud computing security*, 2009, pp. 85–90.

[8] P. Lam, E. Bursztein, and J. Mitchell, "TrackBack Spam: Abuse and Prevention," in *Proceedings of the ACM workshop on Cloud computing security*, 2009.

[9] J. Sobey, T. Whalen, R. Biddle, P. V. Oorschot, and A. Patrick, "Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study," in *Proceedings of the ACM workshop on Cloud computing security*, 2009.

[10] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, "Managing security of virtual machine images in a cloud environment," in *Proceedings of the ACM workshop on Cloud computing security*, 2009, pp. 91–96.

[11] M. Christodorescu, R. Sailer, D. Schales, D. Sgandurra, and D. Zamboni, "Cloud security is not (just) virtualization security: a short paper," in *Proceedings of the ACM workshop on Cloud computing security*, 2009, pp. 97–102.

[12] M. Chase, K. Lauter, J. Benaloh, and E. Horvitz, "Patient Controlled Encryption: patient privacy in electronic medical records," in *Proceedings of the ACM workshop on Cloud computing security*, 2009.

[13] M. Raykova, B. Vo, S. Bellovin, and T. Malkin, "Secure Anonymous Database Search," in *Proceedings of the ACM workshop on Cloud computing security*, 2009.

[14] T. Pering, R. Want, B. Rosario, S. Sud, and K. Lyons, "Enabling pervasive collaboration with platform composition," *Proceedings of Perviasive*, 2009.

[15] K. Lyons, T. Pering, B. Rosario, S. Sud, and R. Want, "Multi-display Composition: Supporting Display Sharing for Collocated Mobile Devices," in *Proceedings of the 12th IFIP TC 13 International Conference on Human-Computer Interaction: Part I*, 2009.

[16] H. XuhuiLi and Y. Zhang, "Deploying Mobile Computation in Cloud Service?" in *Proceedings of the First International Conference for Cloud Computing (CloudCom)*, 2009.

[17] B. Chun and P. Maniatis, "Augmented Smartphone Applications Through Clone Cloud Execution," in *Proceedings of USENIX HotOS XII*, 2009.

[18] X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong, "Securing elastic applications on mobile devices for cloud computing," in *Proceedings of the ACM workshop on Cloud computing security*, 2009, pp. 127–134.

[19] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian, "Virtualized in-cloud security services for mobile devices," in *Proceedings of the First Workshop on Virtualization in Mobile Computing*, 2008, pp. 31–35.

[20] S. Goyal and J. Carter, "A lightweight secure cyber foraging infrastructure for resource-constrained devices," in *Proceedings of the 6th IEEE Workshop on Mobile Computing Systems and Applications*, 2004, pp. 186–195.

[21] J. Lockwood, N. McKeown, G. Watson, G. Gibb, P. Hartke, J. Naous, R. Raghuraman, and J. Luo, "NetFPGA-an open platform for gigabit-rate network switching and routing," in *IEEE International Conference on Microelectronic Systems Education*, 2007.

[22] F. Chong, G. Carraro, and R. Wolter, "Multi-Tenant Data Architecture," Microsoft MSDN Document, available at http://msdn.microsoft.com/en-us/library/aa479086.aspx, 2006.

[23] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *Proceedings of the 28th IEEE Symposium on Security and Privacy (Oakland)*, 2007.

[24] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[25] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal of Computing*, vol. 32, no. 2, pp. 586–615, 2003.

[26] D. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*. Wiley, 2009.

[27] M. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy, "A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks," in *in Proceedings of the IEEE Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MOBIQUITOUS)*, 2005.

[28] T. View, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 2, pp. 305–317, 2006.

[29] S. A. Williams and D. Huang, "Group force mobility model and its obstacle avoidance capability," *Journal of the International Academy of Astronautics, Acta Astronautica*, vol. 65, no. 7-8, pp. 949–957, October-November 2009.

[30] C. E. Perkins, E. M. Belding-Royer, and I. Chakeres, "Ad Hoc On Demand Distance Vector (AODV) Routing," *IETF RFC3561*, October 2003.

[31] D. B. Johnson, Y.-C. Hu, and D. A. M. and, "The dynamic source routing protocol (dsr) for mobile ad hoc networks for ipv4," *IETF RFC4728*, 2007.

[32] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," in *ACM Conference on Computer and Communications Security*, 2009.

[33] M. Musolesi and C. Mascolo, "CAR: Context-Aware Adaptive Routing for Delay-Tolerant Mobile Networks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 2, pp. 246–260, 2009.

[34] C. Mascolo and M. Musolesi, "SCAR: context-aware adaptive routing in delay tolerant mobile sensor networks," in *Proceedings of the 2006 international conference on Wireless communications and mobile computing*. ACM, 2006, p. 538.