**Proceedings of Informing Science & IT Education Conference (InSITE) 2014**

Cite as: Ning, W., Wang, H., & Wang, W. (2014). Security issues on mobile ad hoc network for mobile commerce. *Proceedings of Informing Science & IT Education Conference (InSITE) 2014* (pp. 199-209). Retrieved from http://Proceedings.InformingScience.org/InSITE2014/InSITE14p199-209Ning0568.pdf

# Security Issues on Mobile Ad Hoc Network for Mobile Commerce

***Wei Ning, Haibo Wang, and Wei Wang***
***Sanchez School of Business,***
***Texas A&M International University, Laredo, Texas, USA***

**wei.ning@tamiu.edu; hwang@tamiu.edu; wei.wang@tamiu.edu**

## Abstract

The fifth generation of WiFi and new standards of telecommunication protocols enable the implementation of Mobile ad hoc network in retail business at a lower cost. While the retail industry begins to embrace this new technology and install a WiFi hotspot in their stores and shopping carts, the issues of security become highly challenging to both public and private organizations. This paper will discuss the issues with a systematic approach to address the security of mobile ad hoc network infrastructure. We present some cost efficient but effective solutions to improve the security based on the industrial standards and cutting edge technology.

**Keywords**: security, ad hoc network, mobile commerce

## Introduction

The fifth generation of WiFi and new standards of telecommunication protocols make possible the massive implementation of Mobile Ad Hoc network (MANET) in retail business at a lower cost. While the retail industry have started embracing this new technology and mostly by installing a WiFi hotspot in their stores and shopping carts, the issues of security and reliability become serious concerns to both public and private organizations.

There is a large volume of literature on critical infrastructure of telecommunication system, however, the topic on mobile e-commerce, especially on MANET, still offers researchers many great opportunities for new ideas and designs for transmission of data. This study will present systematic review of the literature on MANET with the objective of addressing security and reliability by studying the state-of-art in MANET research and applications. The authors try to identify the gap between academic and industry, and to point out the challenge and future research directions. We hope that the findings of this study will serve as a good source for whoever is interested in MANET. The paper also presents some real world challenges as well as future research directions.

## M-Commerce and Infrastructure

New technology in telecommunication network infrastructure enable its capability to be spread sparsely over large territories at a global scale, to provide exceptional coverage and to impact the lives of large numbers of people. The new development of Mobile Ad Hoc Network (MANET) communication caught the attention of investigators in both academia and industry. MANET is becoming an industry standard, and some retailers are promoting new customer services powered by MANET technology. The potential applications of MANET will bring a landslide change to the customer relationship management and supply chain management. Thus, the security and reliability of MANET are receiving immediate attentions from both public and private organizations. The advantage and potential applications of MANET in retailing industry include the following: 1) Sharing product information with and bringing online to offline (O2O) experiences to customers. 2) Monitoring the movement of customer in the stores to understand the customer behavior. 3). Enable customer to share shopping experience instantly.  In an environment where other telecommunication networks are unable to perform, the self-organization capability of MANET is the key, in that it can provide the critical communication infrastructure needed to effectively mobilize resources and share information. However, MANET is also vulnerable to destruction and malicious attacks due to its self-organization capability.  Each device (node) in the MANET can act as a router that forwards data packets to other devices (nodes) and forms a very dynamic and unpredictable network topology. The connectivity of MANET depends on many internal and external factors, such as the node's density, the node's count, and lifetime of each node. The routing protocols of the data packet in different layers of MANET are always subject to destruction and attacks. When considering security and reliability of MANET, researchers often raise questions on two important issues: disruption and influence. For example, in the MANET, the attacker can disrupt routing of data packets by short circuiting and taking over the control of multiple nodes using a "wormhole" attack. To prevent such disruption attack, one can identify the critical components of the network by utilizing traffic analysis and building a better protocol for data packet routing. In the influence situation, if the objective is to improve the security and reliability of MANET, one can deploy relay nodes to improve the stability of the network and to reduce energy consumption, which should result in better data packet routing protocols and improved loading schemes for the critical components. However, the two problems often interact and co-exist in many situations. For example, to prevent the "blackhole" attack on MANET, where the attacker pretends to be an authorized node (when authorized nodes are temporary down due to the power outage or battery life) and responds to misroutes data packets to disrupt the network; in this situation, the task is to identify the critical components to promote high availability and minimum downtime for the authorized nodes (lower energy consumption for longer lifetime and less downtime) and to reduce the possibility of compromised networks by creating useful redundancies (relay nodes) to improve the self-healing structure in the MANET.

In addition, unlike other forms of telecommunication network, MANET is extremely mobilized and characterized by complicated configuration.  Other issues such as node hopping, node trustiness and node forward incentive are also needed to be addressed in order to build a reliable MANET for e-commerce. The systematic approach to addressing these issues is to study the critical components in the infrastructure in the real world setting and propose solutions to protect the critical components in a real-time manner. All these tasks require sophisticated algorithms and better network topology. The modeling and analysis of the dependencies and interdependencies among the critical components within the same critical infrastructure system are highly complicated and their behavior is highly nonlinear. Currently, great effort in critical infrastructure management has focused on developing models to simulate the behavior of critical infrastructure systems and to discover the interdependencies and vulnerabilities among the critical infrastructure system.

## *Rising Popularity of MANET in Mobile Commerce*

The concept of mobile commerce was developed in the early stage of mobile technology and many business models were proposed to provide products and services to customer without the limit of the time and location. Tsalgatidou and Pitoura (2001) discussed the business models using hand-held terminals in mobile electronic commerce and transaction issues for these business models defined by the special characteristics of mobile terminals and wireless networks. However, these business models put too much emphasis on the voice and text data, thus bringing limited experience to the customer with high transaction cost due to the bottleneck of bandwidth.

The breakthrough of third and later generation network technology broke the bandwidth limitation on developing mobile commerce and allowed business to promote complex e-commerce interaction with lower transaction cost and higher transmission rate. The rich media and multidimensional interaction between the customers and retailers have added tremendous value to the mobile e-commerce. The development of social network on the mobile platform also prompts retailers to chase innovated business model. Some researchers (Hwang, Consulta, & Yoon., 2007; Kuo & Yu, 2006) investigated the core business models of 3G and 4G service providers and their roles of developing mobile–ecommerce. Recent survey by eDigitalResearch showed that the fast connection on 4G network can accelerate the mobile commerce and enable customer to locate a cheaper product from both online and offline stores by scanning bar codes (eDigitalResearch, 2013). Cloud-based 4G technology can provide customer and retailer a comprehensive platform for interaction and information sharing. In addition, the outdated revenue generation models in the voice service and the declining revenue caused by the intensive competition from service providers, created opportunities for new value-added services built on the next-generation network (NGN) communication platform. The demand of content-rich and multimedia experience from the customer keeps the service providers on enhancing the network bandwidth and transmission rate in order to improve the communication efficiency of mobile commerce. These value-added services not only create new revenue sources for service providers, but also help retailers develop new business strategy. For example, the standard components in the smartphones such as camera and GPS help retailers to deliver products and services to their customers anytime and anywhere; the sharing of information among customer also demonstrates that social group affects individual decisions on purchasing. The availability of MANET infrastructure is a key to deliver these services and to form a social group in the real time.

## Value Creation through Mobile Network

To understand the connection between new value-added services and associated business strategy, Chen and Cheng (2010) reported a study which collected feedback from 35 industry and research institution experts and scholars, using an analytic network process (ANP) method to evaluate the strategy of mobile service providers on the NGN.  The authors presented an evaluation framework for business strategy and discussed how the results of their study can be used as guides for NGN service providers to evaluate, reposition, and improve their service and strategy. In the meantime, Mobile networks provide opportunities for technology-based self-services including e-government services and customer relationship management. Kuo and Chen (2006) presented an analytical tool using the fuzzy synthetic evaluation method based on analytic hierarchy process (AHP) to select and evaluate the best mobile value-added service providers with the most customer satisfaction. The results of this study not only assist consumers to choose the appropriate service providers from the other consumers' opinions but also can help the provider to catch the potential market trend of mobile value-added services based on the prevailing consumer patterns. A recent study by Venkatesh, Chan, and Thong (2012) on a web-based survey of 2,465 citizens showed four key attributes that influenced the adoption and use of the e-government services. One of the key attributes is the security provision.

One of the most attractive value-added services is the mobile banking in e-commerce. The mobile banking breaks the boundary of time and space limitation of commerce activity and lowers the transaction costs comparing to the conventional banking. Many retailers have adopted the mobile banking technology and enhanced their customer services. For example, customers in the Starbuck stores can use their mobile phone to pay for their cups of Java. In many countries, customers can simply use their mobile phones to pay for products and services from soft drinks in the vending machines, to movie theatre tickets. The mobile cash and advanced authorization methods can improve the security of online payment while bring convenience to the customer. The new finger print and face recognition technology in the mobile phone can lower the risk associated with using mobile banking and eliminate the complication of credit card purchase in some business environments. The replacement of lost and misplaced credit card by the customers and the stolen credit card data by the retailers cost businesses millions of dollars every year. In some African countries, conventional Internet banking service is not available due to the lack of infrastructure. Mobile banking can now provide low cost and efficient banking service to the customer and business under such conditions. The project using whitespace spectrum initiated by Google, creates opportunities to the people living in a isolated community by improving their quality of life; the technology lays the foundation for mobile network infrastructure(Welch, 2013). Even in the countries with advanced infrastructure for wired Internet service such as India and China, the conventional money order service is inefficient and inconvenient to customers. Customers spent lots of time in the long waiting lines and shared the high transaction cost. Both countries have large technology-disadvantaged migrant workers population and customers have to visit banks or post offices to send money to their family due to the lack of computer and home internet service. Thus the demand of mobile money transfer creates opportunity for banks and mobile service providers. Singh (2012) reported a study to examine the feasible business model for mobile banking to integrate Indian Post with banking sectors on the mobile communication platform in order to provide efficient and lower cost money transfer services to migration worker. The authors identified the factors for justifying the demand of mobile money order and analyzed the issues of slow adoption of mobile banking. In fact, in many countries, the lack of consumer confidence in security and reliability of mobile platform is the key reason for resistance of slow adoption of mobile banking as a main banking service. The slow implementation of security and reliability strategy by banking sectors cannot keep pace with the development of mobile commerce. In addition, the mobile commerce growth is always related to the development of mobile payment service markets which is still under transition due to the potential new technology innovation for mobile network infrastructure, such as MANET. Dahlberg, Mallat, Ondrus, and Zmijewska (2008) reported a literature review study on the current state of the mobile payment services market. They proposed a framework using a classic model of four contingency and five competitive force factors after analyzing a variety of factors that influence the markets of mobile payment services. They pointed out that the social and cultural factors on mobile payments, as well as comparisons between mobile and traditional payment services, are entirely uninvestigated issues. The directions for future research in this continuing emerging field are discussed.

Another widely developed value-added service is location-based mobile service. The potential of location-based mobile applications and intensive computing demand have attracted the attention from both academy and industry. The hardware and software developers have proposed different mechanism to process the location-dependent queries. The quality of location-based mobile service depends on the efficiency of the queries and the precision of the computing results. Unlike static coordinating online services on the wired internet platform, the location-based mobile services required intensive computing and continuous processing due to the changes of coordinates of customer. For example, to collect the data of customer purchasing behavior inside a retail store, the location-based service need to pinpoint the movement of customers with high precision and record the time spent by the customer on particular items or shelves. The location data in this application will be collected in a fine granularity and precision. To deliver the information on products or services to the customer, based on their locations in such environment, location data need to be refreshed automatically as customers move around the store. It is highly challenging to the service provider on delivering high quality services without draining the battery power of the mobile devices from the customers. MANET can provide a good performance distributed system to process the queries without expensive computing processes. It not only increases the flexibility of network communication and reduces power consumption of the location queries considerably but also performs the location-based service efficiently.  Veijalainen, Terziyan, and Tirri (2006) presents a requirement analysis for the location-based e-commerce transactions using a graphic model based on a Transaction Manager (TM) architecture to protect e-commerce workflows against communication links, applications, or crashes. This system can be applied to monitor constraints related to the security and reliability of critical components in the network.

To provide value-added services to customers, several innovated mobile business models have been proposed. Figge (2004) introduces a situation-dependent service model based on the spatial dimension, personal dimension and temporal dimension of the customer and service provider, this is considered as a situation provider based on the situation description. The author also discussed issues related to organization, technology and security of situation dependency in mobile e-commerce. Huang, Chung, Liu, Lai, and Chen (2009) proposed a hierarchical mobile agent framework for handling key management and access control problems between mobile agent and host. The proposed method can improve the security of key management and mobile control accesses by managing the accessing relationship between the mobile agents and the host, and operate storage space efficiently in a distributed environment, which is important to non-specific network such as MANET.  Jiang, Hu, and Wang (2010) proposed a collaborative business model with optimal profit among the portal access service provider (PASP), the product service provider (PSP), and the mobile service provider (MSP) as a multi-agent system for mobile business. To achieve the optimal profit, the authors presented an agent evolution algorithm (AEA) for computation and used a simulation experiments to show how the decision makers choose the profits-oriented strategies. The results of this study indicated the collaborative mechanism can help players to achieve a better performance at a low level of risk. Esparza, Muñoz, Soriano, and Forné, (2006) discussed the use of mobile agent technology in brokerage systems to accelerate the development of a massive use of mobile e-commerce application and pointed out that security issues that hinder its use. In the next section, we will discuss the security issues related MANET infrastructure in mobile e-commerce.

# Security Issues on MANET

## The Urgent Need for Better MANET Security Solutions

The self-organized nature of MANET infrastructure leads to the vulnerability of security threats and makes it much easier to suffer from numerous attacks than the conventional wired network. In addition, nodes within MANET have unreliable links due to the energy supply and constantly changing topology. All these features make MANET extremely vulnerable to security attacks that exploiting its inherent weakness and this also leads to the proliferation of attacks specifically designed for MANET. Thus, the security concerns for the MANET become prominent given the rising popularity of its application. Park, Ahamed, Susilo, andTaufer (2011) provided a brief overview of the state-of-art research on the security issues on MANET. Datta and Marchang (2012) discussed a wide range of attacks that are of special research importance. In their study, these attacks are divided into two sub-groups: active and passive, determined by the behavioral pattern of such attacks, that is whether they bring disturbance to the function of the network or just intercept key information from this system. They subsequently presented several basic techniques used for protecting MANET from such attacks, most of which are of research importance.

## Attacks Exploiting MANET's Inherent Weakness

The data packets moving among the nodes are controlled by the routing protocol without much security features included. MANET is often characterized by the lack of secured boundaries, Byzantine failure of comprised nodes, absence of centralized management facility, restricted power supply, and poor scalability. For example, the restricted power supply can lead to a Denial of Service (Dos) attack. Researchers classified the attacks on MANET infrastructure as internal and external based on the source and as active and passive based on the behavior. In this section, we discuss the various security issues in MANET infrastructure based on the literature.

First of all, Dos is the common external attack to both wireless and wired network. For example, Ack-storm Dos attacks pose a renewed threat to the network by taking advantage of a flawed-design in TCP specifications. Theoretically, such attack could be amplified by unlimited times and they can be easily initiated in large scale to fight against access network or to block web server even by a very weak MitM attacker. Abramov and Herzberg (2013) found two simple ways to prevent Ack-storm DoS attacks— one through a simple fix in a client or server, the other through a packet-filtering firewall. To prevent Dos attack, Agah, Basu, and Das. (2006) presented a study on the design of security enforcement mechanism through the lens of auction theory. In the new protocol, nodes compete with each other in, "forwarding incoming packets and gaining reputation in the network" on the basis of auction theory. Maximum bids are based on the node's utility value, thus, untruthfully bidding nodes will be identified and therefore isolated in order to prevent DoS attack; this novel protocol is called "Secure Auction based Routing". In addition, the authors discussed the defense strategy in light of game theory. They found that eventually, in a "non-cooperative, two-player, non-zero-sum game between an attacker and a wireless sensor network", the game moves towards Nash Equilibrium, which finally leads to two new strategies. One synthesizes the overall utility of all the en-route nodes in data packet, "where utility is the difference between gain and cost for each node"; the other one utilizes a "rating system" where wireless nodes receive rating from its neighboring nodes. The proposed "game theory based framework" is supported by simulation results in terms of improving defense strategy for the wireless sensor network which is a type of MANET. A more recent attempt to prevent MANET from DoS attacks is done by Jia, Sun, and Stavrou (2013), in which CapMan, a security mechanism based on participating nodes' capability is presented. By its design, CapMan is able to monitor both the capability limit of and the real-time traffic flow through a node. Each node's traffic situation is summarized and exchanged within the whole network. because of this, nodes are able to make informed decision and better regulate the traffic. CapMan is implemented through simulations extensively and the results show that CapMan can effectively thwart even sophisticated DoS attacks.

## Improvements Made on Routing Protocols

In MANET, mobile devices are connected via wireless links. In such a network, nodes change locations very often, thus pose special difficulty for routing algorithm to address the changing topology. Given that there are various protocols available and every protocol is best for a particular setting, Joshi (2011) discusses the security issues and what can be done to address those security issues on Network Layer. Security design is a key function for any type of network. For MANET, which relies on the mobile nodes to accomplish connection and is characterized by dynamic topology, the security design is of special importance. Komninos, Vergados, and Douligeris (2006) discussed the major security issues regarding mobile ad hoc network, "at the data link and network layers", and paid attention to the security requirement in security design for these two layers. Komninos, Vergados, and Douligeris (2007) further investigated the design requirement for MANET in light of multiple authentication protocols and reported a study focusing on the authentication process "in a layered approach". They also performed simulation to test the several such protocols and suggest “multiple lines of defense” to improve the security of MANET infrastructure. In addition,  Shim and Lee (2005) identified the security flaws related to the protocols for authentication and key establishment. Their study revealed a new kind of attack: known key-share attack when the communication protocols in MANET failed to provide authentication. In addition,  Karyotis and Papavassiliou (2007) studied an attack strategy based on a probabilistic model to maximize the disruption caused by those attacks. Considering the dynamic topology of MANET, this proposed model contains a topology control algorithm which is able to evaluate the capability, resources and characteristics of a target network. In so doing, those attacks are expected to cause greater impact on target MANET. The test results show that the proposed algorithm is more effective than, “any other flat and threshold-based approaches”. Adnane, Bidan, and Sousa Júnior, (2013) conducted a comprehensive analysis on the trust based routing protocol-OLSR, presented a detailed review of the reasoning process utilized by node to form a trust value under OLSR protocol, and provided their own modification on the prevailing OLSR protocol. Garcia-Morchon, Kuptsov, Gurtov, and Wehrle (2013) also examined the mechanism of such routing protocols that exercise trust management. Based on their distinct perspective, a modified trust based protocol is proposed in this study which emphasizes the two voting procedures, one for node admission and the other for node elimination. More commonly, building on established and well-performing protocols to make incremental improvement to these protocols is also a practically meaningful approach. von Mulert, Welch, and Seah (2012) presented their Secure AODV protocol, which is built on the established Ad-hoc On-demand Distance Vector (AODV) protocol. Their newly proposed protocol incorporates cryptographic mechanism so as to keep the message transmitted within the network from being “faked” or “altered”.

Given the unstable nature of the nodes in mobile network, there are also protocols designed to address such security issues of MANET. Malavenda, Menichelli, and Olivieri (2012) presented a novel protocol which is delay-tolerant and energy-saving after a thorough exmination of state-of-art protocols of such type. Their proposed protocol have been aproved as good and even outperformed most prevailing mechanism given the experimental results.

Since there are many routing protocols available for security improvement, it is equally important to measure the effectiveness of these porposed protocols so that protocols with better safety parameters could stand out. There are some standards which specify the requirements; such standards include X.800 and X.805. Almomani, Al-Banna, and Al-Akhras (2013) based their analysis on these standards and proposed their logic based security architecture, which can systematically analyze the security requirement a protocol could achieve and give mathematic proof. Based on their proposed architecture, they presented their analysis results for many prevailing protocols.

MANET is considered as a pervasive and ubiquitous network which is vulnerable to internal attack such as the Byzantine failure caused by the compromised nodes. The traditional access control and authentication become inadequate when it comes to pervasive and ubiquitous environment, especially after new technology emerged. To build a reliable pervasive network, Boukerche and Ren (2008) proposed a “reputation-based trust system which assigns credentials to nodes, updates private keys, managing trust value and makes decision”. This system is tested to show that it can effectively identify malicious nodes and take proper action to protect the pervasive network. For the pervasive network, flooding is an effective method when it comes to “secure routing application”. But it also has such flaws as “extreme redundancy”, which often causes broadcast storm and even system failure because of the number of collision. Gossip is “a probabilistic algorithm” used to reduce the number of retransmission by calculating the retransmission probability. Burmester, Le, and Yasinsac (2007) reported a study to reduce the problem of retransmission while retaining as much security as possible by presenting “several new gossip protocols which exploit local connectivity to adaptively correct propagation failures and protect against Byzantine attacks". Because there is no infrastructure in MANET, the communication among nodes is conducted by the nodes themselves. Thus, the cooperation between nodes becomes critical in order to establish a route for communication. For various reasons such as capacities and batteries, some nodes may turn to misbehave and such nodes usually complicate the routing process. Gopalakrishnan and Rhymend Uthariaraj (2012) proposed a solution to mitigate the effect of those misbehaving nodes by introducing a, "Collaborative Polling based Routing Security Scheme" which is effective in detecting and isolating misbehaving nodes. This approach is supposed to reduce false detection. The test results show reduced packet drop ratio and malicious drop. As we move to a ubiquitous computing environment, the risk management becomes more and more critical because of the complexity of the connectivity. Hayat, Reeve, and Boutle (2007) try to find out what effect the traditional information security triangle is going to experience and how the information security requirement is going to be influenced. Special attention has been paid to the need for risk management and "context-based access control" as well as "pro-active threat assessment techniques". Clustering in MANET refers to the method that groups nodes in different clusters. Usually there is a managing node in each cluster; also called "clusterhead". In the current body of knowledge, little concern has been given to the "trust level" of head nodes in the selection process of "clusterhead" for internal attack. Elhdhili, Ben Azzouz, and Kamoun (2008) proposed a clustering algorithm for security in MANET called CASAN, which focuses on the trustworthiness, stability and energy of a potential node. The authors also tested this algorithm through simulation as well as comparison with other clustering techniques; and all these tests show positive evidence in support of CASAN. This approach can be used to identify the critical infrastructure in MANET.

### *Integrative Security Framework*

So far we have discussed the different techniques that one can utilize to strengthen the security of MANET. Since these techniques often have varying focus, grounded in different theoretic basis, and can be applied in different scenarios, thus, many researchers are working on building a integrative framework that incorporate elements from different security strategy to make a comprehensive defense system. Such effort can be illustrated as the framework presented in Lacey et al. (2012). In thus study the authors propose a reputation-based internet protocol security (RIPsec) framework under which links and nodes are encrypted, nodes behavior is monitored and graded under a reputation system, and message exchange is secured by certificate protection. This framework incorporates existing techniques and forms a comprehensive security solution; it is also proved to be more effective against existing attacks based on simulation results. Bankovic et al. (2011) put together a network routing protocol and an intrusion detection system to form a new security solution. This new solution utilizes a reputation based scheme to neutralize its internal threats and leverage an unsupervised algorithm to analyze abnormal behavior, and most importantly, identify attacks that may be unknown beforehand. There are also some frameworks and solution designed specifically for unique situation. The security solution presented in Cionca, Newe, and Dădârlat (2012) provides integrative protection to sensor networks, which are mostly used in hostile environment.

## Challenges and Future Research

In MANET, mobile devices (nodes) are connected via wireless links. In such network, nodes changes locations vary often thus pose special difficulty for routing algorithm to address the changing topology. Given that there are various protocols available and every protocol is best for a particular setting and makes it difficult to choose which protocol to use in the application. It is critical to develop a set of framework to evaluate these protocols in terms of security policy enforcement and efficient transmission of data.

In addition, Mobile technology allows the business and customers to connect at massive scale without time and space boundaries. This capability of mobile commerce will have impacts on the way business happens, for example, mobile technology has already changed the campaign-based consumer marketing strategy to the dialogue-based consumer marketing using social network and encourage consumer to share information. The trusted relationship is not only important for nodes in MANET infrastructure in terms of security and reliability as we discussed early, but also critical to the development of mobile commerce applications between business and customers. The connection oriented nature of mobile communication help to build a much deep trust channel than other connection-less communication, such as email or blog. However, how to develop and maintain the trust in front of increasing malicious attacks is a challenging task to the application developers and service providers.

# References

Abramov, R., & A. Herzberg (2013). TCP Ack storm DoS attacks. *Computers & Security, 33*, 12-27.

Adnane, A., Bidan, C., & de Sousa Júnior, R. T. (2013). Trust-based security for the OLSR routing protocol. *Computer Communications, 36*(10), 1159-1171.

Agah, A., Basu, K., & Das, S. K. (2006). Security enforcement in wireless sensor networks: A framework based on non-cooperative games. *Pervasive and Mobile Computing, 2*(2), 137-158.

Almomani, I., Al-Banna, E., & Al-Akhras, M. (2013). Logic-Based Security Architecture for Systems Providing Multihop Communication. *International Journal of Distributed Sensor Networks,* 2013, 1-17.

Bankovic, Z., Fraga, D., Manuel Moya, J., Carlos Vallejo, J., Malagón, P., Araujo, Á., ... & Nieto-Taladriz, O. (2011). Improving security in WMNs with reputation systems and self-organizing maps. *Journal of Network and Computer Applications, 34*(2), 455-463.

Boukerche, A., & Ren, Y. (2008). A trust-based security system for ubiquitous and pervasive computing environments. *Computer Communications, 31*(18), 4343-4351.

Burmester, M., Le, T. V., & Yasinsac, A. (2007). Adaptive gossip protocols: Managing security and redundancy in dense ad hoc networks. *Ad Hoc Networks, 5*(3), 313-323.

Chen, P.-T. & Cheng, J. Z. (2010). Unlocking the promise of mobile value-added services by applying new collaborative business models. *Technological Forecasting and Social Change, 77*(4), 678-693.

Cionca, V., Newe, T., & Dădârlat, V. T. (2012). Configuration tool for a wireless sensor network integrated security framework." *Journal of Network and Systems Management 20*(3), 417-452.

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications, 7*(2), 165-181.

Datta, R., & Marchang, N. (2012). Chapter 7 - Security for mobile ad hoc networks. In S. K. Das, K. Kant, & Zhang, *Handbook on securing cyber-physical critical infrastructure* (pp.147-190).

eDigitalResearch (2013). Survey finds 4G will accelerate mobile shopping. Retrieved from http://www.edigitalresearch.com/news/item/month/april/year/2013/nid/892198128

Elhdhili, M. E., Ben Azzouz, L., & Kamoun, F. (2008). CASAN: Clustering algorithm for security in ad hoc networks. *Computer Communications, 31*(13), 2972-2980.

Esparza, O., Muñoz, J. L., Soriano, M., & Forné, J. (2006). Secure brokerage mechanisms for mobile electronic commerce. *Computer Communications, 29*(12), 2308-2321.

Figge, S. (2004). Situation-dependent services a challenge for mobile network operators. *Journal of Business Research, 57*(12), 1416-1422.

Garcia-Morchon, O., Kuptsov, D., Gurtov, A., & Wehrle, K. (2013). Cooperative security in distributed networks. *Computer Communications, 36*(12), 1284-1297.

Gopalakrishnan, K., & Rhymend Uthariaraj, V. (2012). Collaborative polling based routing security scheme to mitigate the colluding misbehaving nodes in mobile ad hoc networks. *Wireless Personal Communications, 67*(4), 829-857.

Hayat, Z., Reeve, J., & Boutle, C. (2007). Ubiquitous security for ubiquitous computing. *Information Security Technical Report, 12*(3), 172-178.

Huang, K. H., Chung, Y. F., Liu, C. H., Lai, F., & Chen, T. S. (2009). Efficient migration for mobile computing in distributed networks. *Computer Standards & Interfaces, 31*(1), 40-47.

Hwang, J. S., Consulta, R. R., & Yoon, H. Y. (2007). 4G Mobile Networks–Technology Beyond 2.5 G and 3G. *PTC (Pacific Telecommunications Council) Proceedings*, Hawaii.

Jia, Q., Sun, K., & Stavrou, A. (2013). Capability-Based Defenses Against DoS Attacks in Multi-path MANET Communications. *Wireless personal communications, 73*(1), 127-148.

Jiang, G., Hu, B., & Wang, Y. (2010). Agent-based simulation of competitive and collaborative mechanisms for mobile service chains. *Information Sciences, 180*(2), 225-240.

Joshi, P. (2011). Security issues in routing protocols in MANETs at network layer. *Procedia Computer Science, 3*(0), 954-960.

Karyotis, V. & Papavassiliou, S. (2007). Risk-based attack strategies for mobile ad hoc networks under probabilistic attack modeling framework. *Computer Networks, 51*(9), 2397-2410.

Komninos, N., Vergados, D., & Douligeris, C. (2006). Layered security design for mobile ad hoc networks. *Computers & Security, 25*(2), 121-130.

Komninos, N., Vergados, D. D., & Douligeris, C. (2007). Authentication in a layered security approach for mobile ad hoc networks. *Computers & Security, 26*(5), 373-380.

Kuo, Y.-F., & Chen, P.-C. (2006). Selection of mobile value-added services for system operators using fuzzy synthetic evaluation. *Expert Systems with Applications, 30*(4), 612-620.

Kuo, Y.-F., & Yu, C.-W. (2006). 3G telecommunication operators challenges and roles: A perspective of mobile commerce value chain. *Technovation, 26*(12), 1347-1356.

Lacey, T. H., Mills, R. F., Mullins, B. E., Raines, R. A., Oxley, M. E., & Rogers, S. K. (2012). RIPsec–Using reputation-based multilayer security to protect MANETs. *Computers & Security, 31*(1), 122-136.

Malavenda, C. S., Menichelli, F., & Olivieri, M. (2012). Delay-tolerant, low-power protocols for large security-critical wireless sensor networks. *Journal of Computer Networks and Communication*s, 2012.

Park, J. H., Ahamed, S. I., Susilo, W., & Taufer, M. (2011). Special issue of computer communications on information and future communication security. *Computer Communications, 34*, 223-225.

Shim, K., & Lee, Y.-R. (2005). Security flaws in authentication and key establishment protocols for mobile communications. *Applied Mathematics and Computation, 169*(1), 62-74.

Singh, A. B. (2012). mobile banking based money order for India Post: Feasible model and assessing demand potential. *Procedia - Social and Behavioral Sciences, 37,* 466-481.

Tsalgatidou, A. & Pitoura, E. (2001). Business models and transactions in mobile electronic commerce: Requirements and properties. *Computer Networks, 37*(2), 221-236.

Veijalainen, J., Terziyan, V., & Tirri, H. (2006). Transaction management for m-commerce at a mobile terminal. *Electronic Commerce Research and Applications, 5*(3), 229-245.

Venkatesh, V., Chan, F. K., & Thong, J. Y. (2012). Designing e-government services: Key service attributes and citizens' preference structures. *Journal of Operations Management, 30*(1), 116-133.

Von Mulert, J., Welch, I., & Seah, W. K. (2012). Security threats and solutions in MANETs: A case study using AODV and SAODV. *Journal of Network and Computer Applications, 35*(4), 1249-1259.

Welch, C. (2013). *Google's white spaces trial will beam broadband to ten South African schools*. Retrieved from http://www.theverge.com/2013/3/25/4144946/google-white-spaces-trial-provides-broadband-ten-south-african-schools

## Biographies

**Wei Ning** is now a Ph.D student at Texas A&M International University. His area is international business administration with a concentration in management. He has a bachelor's degree in computer science from Chongqing University of Posts and Telecommunications, China, in 2009, after which he spent three years in completing his MBA degree in University of Detroit, USA. Before being a doctoral student, he has accumulated experience in publishing academic papers by working with faculties from multiple U.S. institutes, with whom he co-authored several academic papers. Wei Ning now is also a research assistant for faculty at TAMIU.

**Haibo Wang** received a Ph. D. in Production Operations Management, 2004 from The University of Mississippi. He is currently associate professor of decision sciences in the Division of International Business and Technology Studies, College of Business Administration at Texas A&M International University. He has received the university scholar of the year award in 2011 and university global scholar of year award in 2013. He is guest professor and visiting professor of a number of institutions in China and guest editors of several international journals. He has publications in such outlets as *European Journal of Operational Research, Journal of Intelligent & Robotic Systems, Computers and Operation Research, IEEE transactions on Control System Technology, IEEE transactions on Automation Science and Engineering, Journal of Operational Research Society, Computers and Industrial Engineering, Journal of Applied Mathematical Modeling, International Journal of Flexible Manufacturing Systems, International Journal of Production Research, Journal of Human and Ecological Risk Assessment, Journal of Heuristics, Communications in Statistics, Journal of Combinatorial Optimization, Journal of Optimization Letters, etc.*

**Wei Wang** is a current student at Texas A&M International University seeking Ph.D in international business administration. She also serves as a research assistant for faculty and has been actively involved in multiple publications and academic conferences. Her research interests include feature selection, critical infrastructure and data mining. Prior to joining TAMIU, she received her Bachelor of engineer from Xi'an Telecommunications Institute in 2006, master's degree of management from Zhongyuan University of Technology in 2009, and her MBA from Texas A&M International University, where she continued pursuing higher education.