TRUST FEATURES-BASED FRIENDSHIP MECHANISM FOR MOBILE AD HOC NETWORKS

NORMALIA BINTI SAMIAN

UNIVERSITI TEKNOLOGI MALAYSIA

TRUST FEATURES-BASED FRIENDSHIP MECHANISM FOR MOBILE AD HOC NETWORKS

NORMALIA BINTI SAMIAN

A thesis submitted in fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

APRIL 2010

ABSTRACT

Mobile Ad hoc Network (MANET) is one of wireless technologies that gains widespread use nowadays. Since ad hoc network does not have fixed infrastructure such as access point that it can rely on, the nodes operate in promiscuous mode and are vulnerable to attacks and service disruption especially from the existence of selfish nodes. This research focuses on how to motivate cooperation and trust among mobile nodes and thwart away malicious nodes without using complex computational process. The goal of this research is to provide a secure mechanism for MANET by enhancing cooperation and trustworthiness among mobile nodes by using friendship mechanism and trust features. The creation of friendship mechanism is inspired from the concept of small-world phenomenon. The main contributions of this research are the enhancement of friendship mechanism's algorithm with trust features and also enhancement of Ad hoc On-demand Distance Vector (AODV) routing protocol's algorithm to gain secure data transmission's path. The definition of secure path in this research is that the path that will be established only consists of nodes that are listed in the trusted friends' list. This means that nodes will not transmit data amongst anonymous nodes that are not listed as trusted friends. All the developed algorithms in this research were demonstrated through Network Simulator 2 (NS-2) software. The results show that although the relationships of trusted nodes are decreased after implementing trust features, it is an acceptable trade off for obtaining more trusted friends and secure paths in AODV. This is proven by the good performances obtained through experiment in terms of packet delivery fraction, normalized routing load and packet loss where under malicious attacks, the proposed work could protect the AODV routing protocol from being severely affected. This research provides a good alternative to secure MANET in such a way that it provides a platform for nodes to exchange information safely in a trusted community.

ABSTRAK

Rangkaian ad hoc bergerak (MANET) merupakan salah satu teknologi tanpa wayar yang digunakan secara meluas pada masa kini. Memandangkan rangkaian ad hoc tidak mempunyai struktur tetap seperti titik capaian sebagai tempat bergantung, nod-nod terlibat akan beroperasi dalam keadaan tidak menentu dan mengakibatkannya mudah terdedah pada serangan dan gangguan perkhidmatan terutamanya dengan kewujudan nod-nod yang mementingkan diri sendiri. Penyelidikan ini memfokus untuk meningkatkan kerjasama dan kepercayaan antara nod-nod bergerak serta menyingkirkan nod-nod tidak baik tanpa menggunakan proses pengkomputeran yang kompleks. Matlamat penyelidikan ini adalah untuk mewujudkan mekanisma keselamatan untuk MANET dengan meningkatkan elemen kerjasama dan kepercayaan antara nod-nod menggunakan mekanisma persahabatan dan ciri-ciri percaya. Pembentukan mekanisma persahabatan diinspirasikan daripada konsep fenomena dunia kecil. Sumbangan utama kajian ini adalah pengukuhan algoritma mekanisma persahabatan menggunakan ciri-ciri percaya dan juga pengukuhan algoritma protokol penghalaan Vektor Jarak Atas-permintaan secara Ad hoc (AODV) untuk mendapatkan laluan penghantaran data yang selamat. Definisi laluan selamat dalam kajian ini adalah laluan tersebut hanya dibina oleh nod-nod yang telah tersenarai sebagai rakan-rakan yang boleh dipercayai. Ini bermakna, nod-nod tidak akan melakukan penghantaran data kepada nod-nod tidak dikenali yang tidak tersenarai sebagai rakan yang boleh dipercayai. Algoritma-algoritma yang dibina telah didemonstrasi menggunakan perisian Pensimulasi Rangkaian 2 (NS-2). Keputusan yang diperolehi menunjukkan bahawa walaupun jumlah hubungan antara nod-nod yang dipercayai berkurangan setelah ciri-ciri percaya diimplementasikan, ia merupakan timbal balik yang boleh diterima untuk mendapat lebih ramai rakan yang boleh dipercayai dan laluan-laluan selamat dalam AODV. Ini dibuktikan melalui prestasi baik yang ditunjukkan dalam eksperimen dari segi kadar penghantaran paket, bebanan penghalaan normal dan kehilangan paket yang mana algoritma cadangan dalam kajian ini dapat melindungi protokol penghalaan AODV daripada mendapat kesan teruk akibat serangan. Penyelidikan ini telah berjaya menyediakan alternatif yang baik dan selamat untuk MANET dengan menyediakan satu platform bagi nod-nod melakukan pertukaran maklumat dengan selamat dalam komuniti yang dipercayai.

ABSTRACT

Mobile Ad hoc Network (MANET) is one of wireless technologies that gains widespread use nowadays. Since ad hoc network does not have fixed infrastructure such as access point that it can rely on, the nodes operate in promiscuous mode and are vulnerable to attacks and service disruption especially from the existence of selfish nodes. This research focuses on how to motivate cooperation and trust among mobile nodes and thwart away malicious nodes without using complex computational process. The goal of this research is to provide a secure mechanism for MANET by enhancing cooperation and trustworthiness among mobile nodes by using friendship mechanism and trust features. The creation of friendship mechanism is inspired from the concept of small-world phenomenon. The main contributions of this research are the enhancement of friendship mechanism's algorithm with trust features and also enhancement of Ad hoc On-demand Distance Vector (AODV) routing protocol's algorithm to gain secure data transmission's path. The definition of secure path in this research is that the path that will be established only consists of nodes that are listed in the trusted friends' list. This means that nodes will not transmit data amongst anonymous nodes that are not listed as trusted friends. All the developed algorithms in this research were demonstrated through Network Simulator 2 (NS-2) software. The results show that although the relationships of trusted nodes are decreased after implementing trust features, it is an acceptable trade off for obtaining more trusted friends and secure paths in AODV. This is proven by the good performances obtained through experiment in terms of packet delivery fraction, normalized routing load and packet loss where under malicious attacks, the proposed work could protect the AODV routing protocol from being severely affected. This research provides a good alternative to secure MANET in such a way that it provides a platform for nodes to exchange information safely in a trusted community.

ABSTRAK

Rangkaian ad hoc bergerak (MANET) merupakan salah satu teknologi tanpa wayar yang digunakan secara meluas pada masa kini. Memandangkan rangkaian ad hoc tidak mempunyai struktur tetap seperti titik capaian sebagai tempat bergantung, nod-nod terlibat akan beroperasi dalam keadaan tidak menentu dan mengakibatkannya mudah terdedah pada serangan dan gangguan perkhidmatan terutamanya dengan kewujudan nod-nod yang mementingkan diri sendiri. Penyelidikan ini memfokus untuk meningkatkan kerjasama dan kepercayaan antara nod-nod bergerak serta menyingkirkan nod-nod tidak baik tanpa menggunakan proses pengkomputeran yang kompleks. Matlamat penyelidikan ini adalah untuk mewujudkan mekanisma keselamatan untuk MANET dengan meningkatkan elemen kerjasama dan kepercayaan antara nod-nod menggunakan mekanisma persahabatan dan ciri-ciri percaya. Pembentukan mekanisma persahabatan diinspirasikan daripada konsep fenomena dunia kecil. Sumbangan utama kajian ini adalah pengukuhan algoritma mekanisma persahabatan menggunakan ciri-ciri percaya dan juga pengukuhan algoritma protokol penghalaan Vektor Jarak Atas-permintaan secara Ad hoc (AODV) untuk mendapatkan laluan penghantaran data yang selamat. Definisi laluan selamat dalam kajian ini adalah laluan tersebut hanya dibina oleh nod-nod yang telah tersenarai sebagai rakan-rakan yang boleh dipercayai. Ini bermakna, nod-nod tidak akan melakukan penghantaran data kepada nod-nod tidak dikenali yang tidak tersenarai sebagai rakan yang boleh dipercayai. Algoritma-algoritma yang dibina telah didemonstrasi menggunakan perisian Pensimulasi Rangkaian 2 (NS-2). Keputusan yang diperolehi menunjukkan bahawa walaupun jumlah hubungan antara nod-nod yang dipercayai berkurangan setelah ciri-ciri percaya diimplementasikan, ia merupakan timbal balik yang boleh diterima untuk mendapat lebih ramai rakan yang boleh dipercayai dan laluan-laluan selamat dalam AODV. Ini dibuktikan melalui prestasi baik yang ditunjukkan dalam eksperimen dari segi kadar penghantaran paket, bebanan penghalaan normal dan kehilangan paket yang mana algoritma cadangan dalam kajian ini dapat melindungi protokol penghalaan AODV daripada mendapat kesan teruk akibat serangan. Penyelidikan ini telah berjaya menyediakan alternatif yang baik dan selamat untuk MANET dengan menyediakan satu platform bagi nod-nod melakukan pertukaran maklumat dengan selamat dalam komuniti yang dipercayai.

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	-	Ad hoc On-demand Distance Vector
ARAN	-	Authenticated Routing for Ad hoc Network
AWK	-	AWK is derived from the surnames of its authors – Alfred Aho, Weinberger, and Brian Kernighan.
BSS	-	Basic Service Set
CA	-	Certificate Authority
CBR	-	Constant Bit Rate
CPU	-	Central Processing Unit
DoS	-	Denial of Service
DSDV	-	Destination Sequenced Distance Vector
DSR	-	Dynamic Source Routing
ESS	-	Extended Service Set
GUI	-	Graphical User Interface
IBSS	-	Independent Basic Service Set
IDS	-	Intrusion Detection System
IEEE	-	Institute of Electrical and Electronics Engineers
IETF	-	Internet Engineering Task Force

LL	-	Traditional Link Layer
MAC	-	Media Access Control
MANET	-	Mobile Ad hoc Network
MIT	-	Massachusetts Institute of Technology
NAM	-	Network Animator
NED	-	NEtwork Description
NS-2	-	Network Simulator 2
OPNET	-	Optimized Network Engineering Tools
OTcl	-	Object Tcl
PDF	-	Packet Delivery Fraction
PHY	-	Physical Layer
PKG	-	Private Key Generator
PKI	-	Public Key Infrastructure
QoS	-	Quality of Service
RAM	-	Random Access Memory
RFC	-	Request For Comments
RREP	-	Route Reply
RREQ	-	Route Request
RRER	-	Route Error
SEAD	-	Secure Efficient Distance Vector Routing
SAODV	-	Secure Ad hoc On-demand Distance Vector
TARP	-	Trust Aware Routing Protocol
TCP	-	Transmission Control Protocol
TTL	-	Time To Live
UDP	-	User Datagram Protocol

WAP	-	Wireless Application Protocol
WiMAX	-	Worldwide Interoperability for Microwave Access
WLAN	-	Wireless Local Area Network
WMN	-	Wireless Mesh Network
WPAN	-	Wireless Personal Area Network
WSN	-	Wireless Sensor Network
ZRP	-	Zone Routing Protocol

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

The advancement in telecommunication technologies has brought up the emergence of popular wireless local area network (WLAN). WLAN has proven to be one of a very good way of communications without the use of wires. Currently, people have been moving towards these kinds of communication methods due to their ability to connect people in a more flexible way. WLAN can be classified into two major categories: networks that have a fixed infrastructure and networks that do not have any fixed infrastructure. The latter, which is also known as a mobile ad hoc network (MANET) will be the focus of this study.

A MANET consists of autonomous mobile nodes that are free to roam arbitrarily with no centralized controller such as router to determine the communication paths.

Each node in the ad hoc network has to rely on each other in order to forward packets. Every node can operate both as a host and a router at a time, thus there is a need to deploy a suitable routing protocol to assist nodes in forwarding packets across the network. Examples of MANET's routing protocols are Ad hoc On-demand Distance Vector (AODV), Zone Routing Protocol (ZRP), Destination Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR) (Pandey *et al.*, 2005). These routing protocols work using different techniques but the major similar contribution is to find the shortest path in the source-destination routes selection. Significant applications of MANET range from critical situation such as in military battlefield and emergency medical operation to simple usage like file sharing between business associates and interaction between students and lecturers in classrooms.

The nature of MANET communication that utilizes wireless link has put such a network into facing several passive and active attacks. These attacks could come from several ways including from internal and external intruders. Nodes could easily be compromised or controlled by attackers if there is no secure mechanism to protect them. The approach to secure MANET should be different than those that have been used in wired networks due to the different characteristics of both networks.

There are many approaches have been proposed by researchers to enhance security in MANET. In the works done by Zhang *et al.* (2003) and Boukerche (2006), four different approaches had been lined out to solve the security issues in ad hoc networks: intrusion detection, secure routing, service availability protection, and trust and key management service. An intrusion detection system acts as a defensive technique to thwart away attacks by monitoring activities in the network and generate reports whether certain system is under attack or not. Secure routing on the other hand is a method to protect MANET at the routing protocol level from internal and external attacks. The most common mechanism to secure routing protocols is by using cryptographic techniques (Li *et al.*, 2006). However, due to the increasing number of new attacking techniques, cryptographic mechanism is no longer relevant to be the sole solution in protecting MANET's routing protocols. There is a need to enhance the current solution with more effective approaches that can still tolerate with the dynamic nature of MANET. The third approach which is service availability protection is an approach of solving the unavailability service problem in MANET that is caused by selfish nodes. There are two commonly used approaches: reputation-based and monitoring approach which will be further described in Chapter 2. The last approach of securing MANET (i.e. trust and key management service) is the service required by cryptographic mechanisms to create a mutual trust among nodes. In such an approach, each node holds a key issued by the certificate authority (CA) that controls the process of key revocation and renewal.

Although many solutions have been proposed to increase security element in MANET, there are still ample rooms to make improvements. As MANET is currently becomes more significant and widely used in many applications, it is important to tackle arising security issues that exist so that the technology could functions effectively. Hence, the purpose of this research is to investigate security issues that exist in MANET and study on focusing issues prior to coming up with proposed solutions.

1.2 Background and Motivation

An ad hoc network possesses several characteristics that make it more vulnerable to attacks compared to wired network. The network topology of a MANET is dynamic in nature in which mobile hosts hold arbitrary way of movement and do not have fixed physical locations. The network is decentralized and every node plays multiple roles in discovering routes and forwarding packets. Due to the mobility feature of each node, the network topology may have to face rapid changes as frequent as possible over time which needs efficient routing protocol to control the activities of the nodes. According to Ghosh *et al.* (2005), although efficient routing protocols like AODV and DSR have been introduced, these protocols are prone to attacks that come in several ways and forms especially when it comes to dealing with malicious nodes.

There are several attacks that are well known as being major threats to MANET such as forging legitimate data packets to cause the real data to be sent to the wrong destination (blackhole) (Cooke *et al.*, 2004), injection of a large number of unnecessary routing updates that will consume network bandwidth and router processing time (Hu *et al.*, 2002), and packet forwarding from malicious nodes (Ghosh *et al.*, 2005). However, the security techniques that have been proposed for wired networks cannot be implemented in an ad hoc network due to the difference requirements of both networks such as cost, power consumption, behavior of network topology, computational abilities and Quality of Service (QoS) (Hu *et al.*, 2004).

The susceptibilities of MANET have drawn attentions from many researchers to develop security mechanisms to overcome the problems. Many of the solutions are related to providing a more secure protection on routing protocol based on authentication mechanism. For instance, an extension to AODV routing protocol called Secure AODV (SAODV) has been proposed by Zapata (2006). This work combines the use of both asymmetric and symmetric keys by appending RSA key and hash chain on the messages. The fact that this work utilizes both public and private cryptography keys imposes the nodes in the network to high processing overhead and with so many unrealistic assumptions; the SAODV approach is actually only suitable for best case scenario. Hu *et al.* (2002) have proposed a Secure Efficient Distance Vector Routing (SEAD) that uses a symmetric cryptographic technique called one-way hash functions. In comparison with asymmetric cryptographic, even though the symmetric technique provides less complex computational process, it is still facing an increasing amount of overhead problem in the network resulting from the authentication process. Other authentication-based security mechanisms have been proposed in (Marti *et al.*, 2000; Smith *et al.*, 1997). Similar to SEAD, these approaches face the risk of having higher computational overhead and delay. Besides, they also have a tendency to find the shortest path between source and destination but at the same time ignoring the possibility of colluding malicious nodes in the route selection process.

A common problem that occurs in MANET due to its autonomous characteristic is the selfish behavior of certain involving nodes that are motivated by their intention to conserve their own limited resources such as time, energy and bandwidth (Karygiannis *et al.*, 2006; *Yokoyama et al., 2006*). In MANET environments that rely heavily on nodes' participation, the existence of non-cooperative nodes would affect the successful of a packet transmission. Since the problem is caused by the authorized internal nodes, even with the deployment of the best cryptographic mechanism will not solve the problem. The act of selfishness is mostly driven by the lack of trust among each node. Trust plays an important factor for nodes to cooperate with each other. However, it is not easy to make each node to trust each other as trust is a very subjective matter that cannot be simply fostered using certain fixed rules. Thus, there is a need to propose a solution that could encourage trust and cooperation among mobile nodes other than using traditional authentication schemes. The issue with current security implementation by using cryptographic scheme is that it uses a lot of device's resources due to complex computational process and causing the production of high overhead in the network. As a result, more selfish nodes problem will occur.

Having the discussed issues as motivation, it is important to provide a suitable security solution that could reduce the number of uncooperative mobile nodes by having trusted nodes community.

REFERENCES

Abdul-Rahman, A. and Hailes, S. (1997). A distributed trust model. *Proceedings of New Security Paradigms Workshop (NSPW '97)*. 23-26 September. Great Langdale, Cumbria, UK, 48–60.

Abolhasan, M., Wysocki, T. and Dutkiewicz, E. (2004). A Review of Routing Protocols for Mobile Ad hoc Networks. *Ad Hoc Networks*. Vol. 2, 1-22.

Abusalah, L., Khokhar, A., BenBrahim, G. and ElHajj, W. (2006). TARP: Trust-Aware Routing Protocol. *Proceedings of the 2006 International Conference on Communications and Mobile Computing (IWCMC)*. 3-6 July. Vancouver, British Columbia, Canada, 135 – 140.

Alaoui, A., Quintero, A. and Ivascu, G. I. (2008). Hybrid Routing Protocol with Quality of Service Support for Ad Hoc Wireless Networks. *International Journal of Ad Hoc and Ubiquitous Computing*. 3(2), 111-121.

Andel, T. R. and Yasinac, A. (2006). On the Credibility of Manet Simulations. *IEEE Computer Magazine*. 39(7), 48-54.

Boukerche, A. (2006). *Handbook of Algorithms for Wireless Networking and Mobile Computing*. USA: Chapman and Hall/CRC Press.

Britsocat. (1995). "Number of Close Friends". http://www.britsocat.com/BodySecure.aspx?control=BritsocatMarginals&var=PALS&SurveyID=224

Broch, J., Maltz, D. A, Johnson, D. B., Hu, Y.-C. and Jetcheva, J. (1998). A Performance Comparison of Multihop Wireless Ad hoc Network Routing Protocols. *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*. Dallas, Texas, United States, 85-97.

Cabrera, A. T. and Casilari, E. (2006). Network Simulator: A Learning Tool for Wireless Technologies. In Méndez-Vilas, A. (Ed.). *Current Developments in Technology-Assisted Education*, (3:1979–1983). Seville, Spain: FORMATEX.

Cooke, E., Bailey, M., Mao, Z. M., Watson, D., Jahanian, F. and McPherson, D. (2004). Towards Understanding Distributed Blackhole Placement. *Proceedings of the 2004 ACM workshop on Rapid Malcode*. 29th October. Washington DC, USA, 54-64.

Deng, H., Mukherjee, A. and Agrawal, D. P. (2004). Threshold and Identity-based Key Management and Authentication for Wireless Ad hoc Networks. *Proceedings of the IEEE International Conferences on Information Technology (ITCC'04)*. 5-7 April. Las Vegas, Nevada, 107-111.

Dhakan, P. and Menezes, R. (2005). The Role of Social Structures in Mobile Ad Hoc Networks. *Proceedings of 43rd ACM Southeast Conference*. 18-20 March. Kennesaw, GA, USA, 59-64.

Eschenauer, L. (2002). *On Trust Establishment in Mobile Ad-Hoc Networks*. Master's Thesis, Department of Electrical and Computer Engineering, University of Maryland.

Garg, N. and Mahapatra, R. P. (2009). MANET Security Issues. *International Journal of Computer Science and Network Security (IJCSNS)*. 9(8), 241-246.

Gasser, M., Goldstein, A., Kaufman, C. and Lampson, B. (1989). The Digital Distributed Systems Security Architecture. *Proceedings of the 12th National Computer Security Conference*. 10-13 October. Baltimore, MD USA, 305-319.

Ghosh, J., Philip, S. J. and Qiao, C. (2004). Acquaintance Based Soft Location Management (ABSLM) in MANET. *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'04).* 21st-25th March. 166-171.

Ghosh, T., Pissinou, N. and Makki, K. (2005). Towards Designing a Trusted Routing Solution in Mobile Ad Hoc Networks. *Journal of Mobile Networks and Applications*. Vol. 10(6), 985 – 995.

Guare, J. (1990). *Six Degrees of Separation: A Play*. New York: Vintage Books.

Hardin, G. (1968). The Tragedy of the Commons. *Science.* 162, 1243–1248.

Helmy, A. (2003). Small Worlds in Wireless Networks. *Journal of the IEEE Communications Letters*. 7(10), 490-492.

Hong, X., Xu, K. and Gerla, M. (2002). Scalable Routing Protocols for Mobile Ad hoc Networks. *IEEE Network*. 14(4), 11-21.

Hu, Y. C. and Johnson, D. B. (2004). Secure Routing in Ad hoc Networks: Securing Quality-of-Service Route Discovery in On-demand Routing for Ad hoc Networks. *Proceedings of the 2nd ACM Workshop on Security of Ad hoc and Sensor Networks (SASN '04)*. 25th October. Washington DC, USA, 106-117.

Hu, Y. C., Johnson, D. B. and Perrig, A. (2002). SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02)*. 20-21 June. Calicoon, NY USA, 3-13.

Hu, Y. C., Perrig, A. and Johnson, D. B. (2002). Ariadne: A Secure On Demand Routing Protocol for Ad Hoc Networks. *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02)*. 23-28th September. Atlanta, Georgia USA, 12-23.

Jain, R. (1991). *The Art of Computer Systems Performance Analysis Techniques for Experimental Design, Measurement, Simulation, and Modeling.* (1st ed.) New York: John Wiley and Sons, Inc.

Jamali, M. and Abolhassani, H. (2006). Different Aspects of Social Network Analysis. *Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence WI '06.* 18-22 December. Hong Kong, 66-72.

Jonker, C.M. and Treur, J. (1999). Formal Analysis of Models for the Dynamics of Trust Based on Experiences. *Proceedings of the 9th European Workshop on Modeling Autonomous Agents in a Multi-Agent World: Multi-Agent System Engineering (MAAMAW'99)*. 30th June-2nd July. Valencia, Spain, 221-231.

Kant, K. (1992). *Introduction to computer system performance evaluation*. New York: McGraw-Hill.

Karygiannis, A., Antonakakis, E., and Apostolopoulos, A. (2006). Detecting Critical Nodes for MANET Intrusion Detection Systems. *In Proceedings of Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU'06)*. 29 June. Lyon, France, 9-15.

Kleinberg, J. (2000). The Small-world Phenomenon: An Algorithm Perspective. *Proceedings of the thirty-second annual ACM symposium on Theory of computing STOC '00*. 21-23 May. Portland, Oregon, United States, 163-170.

Kong, J., Zerfos, P., Luo, H., Lu, S. and Zhang, L. (2001). Providing Robust and Ubiquitous Security Support for Mobile Ad-hoc Networks. *Proceedings of the IEEE 9th International Conference on Network Protocols (ICNP'01)*. 11-14 November. Riverside, California, USA, 251-260.

Li, H. and Singhal, M. (2006). A Secure Routing Protocol for Wireless Ad Hoc Networks. *Proceedings of the 39th Hawaii International Conference on System Sciences*. 4-7 January. Hawaii, USA, 225-234.

Liu, J., Yuan, Y., Nicol, D. M., Gray, R. S., Newport, C. C., Kotz, D. and Perrone, L. F. (2004). Simulation Validation using Direct Execution of Wireless Ad-Hoc Routing Protocols. *Proceedings of the 18th Workshop on Parallel and Distributed Simulation (PADS '04)*. Kufstein, Austria, 7-16.

Marker, J. P. and Corson, M. S. (2006). Mobile Ad Hoc Networking and the IETF. *Journal of ACM SIGMOBILE Mobile Computing and Communications Review*. 10 (1), 58-60.

Marsh, S. P. (1994). *Formalising Trust as a Computational Concept*. Ph.D. Thesis. Department of Computing Science and Mathematics, University of Stirling.

Marti, S., Giulli, T. J., Lai, K. and Baker, M. (2000). Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *Proceeding of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*. 6-11 August. Boston, Massachusetts, United States, 255-265.

Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Journal Academy of Management Executive*. 20(3), 709-734.

Michiardi, P. and Molva, R. (2002). Simulation-based Analysis of Security Exposures in Mobile Ad hoc Networks. *Proceedings of European Wireless Conference*. 25-28 February. Firenze, Italy.

Milgram, S. (1967). The small world problem. *Journal of Psychology Today. Vol.* 2, 60-67.

Miranda, H. and Rodrigues, L. (2003). Friends and Foes: Preventing Selfishness in Open Mobile Ad Hoc Networks. *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03)*. 19th-22nd May. Providence, Rhode Island, USA, 440-450.

Musolesi, M., Hailes, S. and Mascolo, C. (2004). An Ad hoc Mobility Model Founded on Social Network Theory. *Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '04)*. 4-6 October. Venice, Italy, 20-24.

Nekkanti, R. K. and Lee, C. (2004). Trust Based Adaptive on Demand Ad hoc Routing Protocol. *Proceedings of the 42nd Annual Southeast Regional Conference*. 2-3 April. Huntsville, Alabama, 88-93.

Osipov, E. and Tschudin, C. (2006). Evaluating the Effect of Ad hoc Routing on TCP Performance in IEEE 802.11 Based MANETs. Proceedings of the 6th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN '06). St. Petersburg, Russia, 298-312.

Pandey, A. K. and Fujinoki, H. (2005). Study of MANET Routing Protocols by GloMoSim Simulator. *International Journal of Network Management*. 15(6): 393–410.

Perkins, C. E. and Belding-Royer, E. M. (1999). Ad-hoc On-demand Distance Vector Routing. *Second IEEE Workshop on Mobile Computing Systems and Applications*, 90-100.

Pirzada, A. A. and McDonald, C. (2004). Establishing Trust in Pure Ad-hoc Networks. *Proceedings of the 27th Conference on Australasian Computer Science (CRPIT '04)*. January. Dunedin, New Zealand, 47-54.

Razak, S. A. (2007). *Two-Tier Intrusion Detection System for Mobile Ad Hoc Network*. Ph.D. Thesis. School of Computing, Communications & Electronics, University of Plymouth.

Reddy, D., Riley, G.F., Larish, B. and Chen, Y. (2006). Measuring and Explaining Differences in Wireless Simulation Models. *Proceedings of the 14th IEEE International Symposium on Modeling, Analysis, and Simulation (MASCOTS '06),* 11-14 September. Monterey, California, USA, 275-282.

Richardson, M., Agrawal, R. and Domingos, P. (2003). Trust management for the Semantic Web. *Lecture Notes in Computer Science*, Vol. 2870, 351-368.

Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B. N., Shields, C. and Belding-Royer, E. M. (2002). A Secure Routing Protocol for Ad Hoc Networks. *Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02)*. 12-15 November. Paris, France, 78-89.

Smith, B., Murthy, S. and Garcia-Luna-Aceves, J. (1997). Securing Distance Vector Routing Protocol. *Proceedings of the Symposium on Network and Distributed System Security (SNDSS'97)*. 10-11 February. San Diego, CA, USA, 85-92.

Stakhanova, N., Basu, S., Zhang, W., Wang, X. and Wong, J. (2007). Specification Synthesis for Monitoring and Analysis of MANET Protocols. *International Symposium on Frontiers in Networking with Applications (FINA 2007)*. 21-23 May. Niagara Falls, On, Canada, 183-187.

Stallings, W. (1999). *Cryptography and Network Security: Principles and Practice*. New York: Prentice-Hall.

Theodorakopoulos, G. and Baras, J. S. (2004). Trust Evaluation in Ad Hoc Networks. *Proceedings of the 2004 ACM Workshop on Wireless Security (WiSe '04)*. 1st October. Philadelphia, PA, USA, 1-10.

Varga, A. and Hornig, R. (2008). An Overview of the OMNeT++ Simulation Environment. *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops (SIMUTools '08)*. 3-7 March. Marseille, France, 1-10.

Venkataraman, R. and Pushpalatha, M. (2006). Security in Ad Hoc Networks: An Extension of Dynamic Source Routing In Mobile Ad Hoc Networks. *Proceedings of the 10th IEEE Singapore International Conference on Communication Systems (ICCS 2006)*. October. Singapore, 1-5.

Weingartner, E., Lehn, H. V. and Wehrle, K. (2009). A Performance Comparison of Recent Network Simulators. *Proceedings of the IEEE International Conference on Communications (ICC 2009)*. 14-18 June. Dresden, Germany, 1-5.

Xian, X., Shi, W. and Huang, H. (2008). Comparison of OMNET++ and Other Simulator for WSN Simulation. *Proceedings of the 3rd IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 3-5 June. Singapore, 1439-1443.

Yan, Z., Zhang, P. and Virtanen, T. (2003). Trust Evaluation Based Security Solution in Ad Hoc Networks. *Proceedings of the 7th Nordic Workshop on Secure IT Systems, NordSec 2003*. October. Gjovik, Norway, 1-14.

Yang, H., Luo, H., Ye, F., Lu, S. and Zhang, L. (2004). Security in mobile ad hoc networks: Challenges and solutions. *Journal of IEEE Wireless Communications*. 11 (1), 38-47.

Yang, T. A. and Zahur, Y. (2005). *Security in Wireless Local Area Networks*. In Ilyas, M. and Ahson, S. *Handbook of Wireless Local Area Networks: Applications, Technology, Security, and Standards*. (425-446). USA: CRC Press.

Yokoyama, S., Nakane, Y., Takahashi, O., and Miyamoto, E. (2006). Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods. *In Proceedings of 7th International Conference on Mobile Data Management (MDM'06)*. 10-12 May. Nara, Japan, 95-100.

Zahur, Y. and Yang, T. A. (2004). Wireless LAN Security and Laboratory Designs. *The Journal of Computing Sciences in Colleges*. 19(3), 44-60.

Zapata, M. G. (2006). Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. Internet Draft: draft-guerrero-manet-saodv-06.txt. Work in Progress.

Zhang, W., Rao, R., Cao, G. and Kesidis, G. (2003). Secure Routing in Ad Hoc Networks and a Related Intrusion Detection Problem. *IEEE Military Communications Conference (MILCOM)*. 13-16 October. Monterey, CA. USA, 735-740.

Zhang, Y. and Lee, W. (2000). Intrusion Detection in Wireless Ad-Hoc Networks. *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom)*. 6-11 August. Boston, Massachusetts, USA, 275-283.

Zhou, L. and Haas, Z. J. (1999). Securing Ad Hoc Networks. *Journal of IEEE Network*. 13(6), 24-30.