NEW FRAMEWORK FOR SECURING MOBILE ADHOC NETWORK USING LIGHTWEIGHT AUTHENTICATION AND SIGNATURE-BASED INTRUSION DETECTION SYSTEM

SATRIA MANDALA

UNIVERSITI TEKNOLOGI MALAYSIA

NEW FRAMEWORK FOR SECURING MOBILE ADHOC NETWORK USING LIGHTWEIGHT AUTHENTICATION AND SIGNATURE-BASED INTRUSION DETECTION SYSTEM

SATRIA MANDALA

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JULY 2012

To my parents, my wife (Ary Nur Azizah), and my sons (Thariq, Zaki, and Farid), I love you all

ACKNOWLEDGMENT

All prays be to God, Allah. Without His mercy and clemency nothing would have been possible. First and foremost, I would like to express my gratitude to my main supervisor, Prof. Dr. Abdul Hanan Abdullah, for encouragement, guidance and critics throughout my graduate studies. It is difficult to find supervisor that always allocate the time for listening to the little problems and roadblocks that unavoidably appear in the performing research. I am also very thankful to both of my co-supervisors, Associate Prof. Dr. Md. Asri Ngadi and Prof. Dr. Abdul Samad bin Haji Ismail, for their guidance, advices, motivation and friendship. Their technical and editorial advice was essential to the completion of my thesis and taught me innumerable lessons and insights while working on my academic research.

I would like to thank Ministry of Science, Technology & Innovation, Malaysia for supporting research funding of my study. I would also like to thank Professor Douglas Lea from State University of New York at Oswego, Dr. Suhartono from ITS, Indonesia, and Assistant Professor Loukas Lazos from University of Arizona, for inspiring discussion given throughout my study. They gave me feedbacks on my ideas and experiment results. I owe some colleagues and friends lots of thanks for their help and contribution. I would mention they are Miss Maznah Kamat and Saiful Adly. I should recognize their support.

I am grateful to all my family members, especially my mother Ramilah and in the memory of my father M.H. Soebakti, who set the example and who made me who I am. I am also deeply indebted to my wife, Ary Nur Azizah for her unconditional love and support throughout my whole life. Special thank you to my sons, Thariq, Zaki, and Farid, who have inspired me to keep on striving to complete the study. Finally, I would like to express my deep gratitude to my guru, Prof. Dr. Abdul Hanan Abdullah, Associate Prof. Daut bin Daman, and Prof. Dr. Abdul Samad bin Haji Ismail for their wisdom and encouragement to help me complete this work.

ABSTRACT

Mobile Adhoc Network (MANET) is vulnerable to network attacks due to its open communication medium. Blackhole and wormhole attacks are the most severe attacks in the network. The attacks cause congestion and increase the possibility of confidential data theft. Unfortunately, the existing security solutions are insufficient to protect the network. This work proposed a new security framework, named Extra Secure Adhoc on Demand Distance Vector (ESAODV). This framework provides a defense-in-depth protection through layered security measures: secure protocol and intrusion detection system (IDS) with extra countermeasures. The first layer implements lightweight packet authentication, and the second layer monitors and counters malicious packets. In this study, ESAODV was implemented using Java in Time Simulator/Scalable Wireless Adhoc Network Simulator, and analyzed using R-Statistics, Sigma Plot and Minitab. Results showed that ESAODV had contained the blackhole attack and the hybrid blackhole attack (HBHA) effectively. The number of corrupting routing tables of benign nodes could be minimized to be near zero even if the number of attackers were increased. In addition, the IDS accurately detected the wormhole and the variant of wormhole attack called diversion of packet over the wormhole link (DP-WHL). The false positive for live attack detection was small. The accuracy of detection was more than 94.5 percent. Although attackers changed the pattern of packets diversion, the IDS detected the new attack pattern in near real time. In addition to these findings, this research has also modeled four performance metrics data of ESAODV, i.e., memory usage, elapsed time for completing routing tasks, number of route replies and route success, based on both linear regression and neural network. Goodness of fit parameters for the models based on the neural network was higher than the linear regression. ESAODV has been proven to provide a comprehensive protection from the most severe attacks in the network. Furthermore, the performance metrics of ESAODV based on the neural network produced a superior model.

ABSTRAK

Rangkaian mudah alih *adhoc* (MANET) terdedah kepada serangan rangkaian kerana medium komunikasinya terbuka. Serangan *blackhole* dan *wormhole* adalah serangan yang paling bahaya dalam rangkaian MANET. Serangan ini menyebabkan kesesakan dalam rangkaian dan meningkatkan kemungkinan kecurian data sulit. Malangnya, penyelesaian keselamatan yang sedia ada tidak mencukupi untuk melindungi rangkaian tersebut. Kerja ini mencadangkan satu rangka kerja baru yang dinamakan sebagai *Extra Secure Adhoc on Demand Distance Vector* (*ESAODV*). Rangka kerja ini memberikan perlindungan pertahanan secara mendalam melalui langkah-langkah keselamatan berlapis: protokol keselamatan dan sistem pengesanan pencerobohan (IDS) dengan langkah balas tambahan. Lapisan pertama melaksanakan pengesahan paket yang ringan, dan lapisan kedua memantau dan membalas paket jahat. Dalam kajian ini, ESAODV telah diterapkan menggunakan *simulator* JiST/SWANS dan dianalisis menggunakan R-Statistics, Sigma Plot dan perisian Minitab. Keputusan menunjukkan, ESAODV boleh membendung serangan *blackhole* dan *hybrid blackhole attack* (HBHA) dengan berkesan. Kerosakan kandungan jadual penghalaan pada nod benigna dikurangkan kepada hampir sifar walaupun bilangan penyerang meningkat. Selain daripada itu, IDS boleh mengesan dengan tepat *wormhole* dan variasi serangan *wormhole* yang dikenali sebagai DP-WHL. Pengesanan positif palsu untuk serangan ini adalah kecil. Ketepatan pengesanan adalah tinggi iaitu melebihi 94.5 peratus. Walaupun penyerang mengubah corak pengalihan paket, IDS mengesan corak serangan tersebut kepada masa nyata. Selain daripada itu, kajian ini juga telah memodelkan empat data metrik prestasi ESAODV seperti penggunaan memori, masa yang diambil untuk menyelesaikan tugasan penghalaan, bilangan jawapan halaan dan halaan yang berjaya berdasarkan regresi linear dan rangkaian neural. Parameter ketepatan padanan bagi model berdasarkan rangkaian neural adalah lebih tinggi daripada regresi linear. ESAODV telah terbukti menyediakan perlindungan komprehensif daripada serangan yang paling bahaya dalam rangkaian ini. Tambahan lagi, metrik prestasi ESAODV berdasarkan rangkaian neural menghasilkan satu model yang unggul.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	–	Adhoc On Demand Vector
ARAN	–	Authenticated Routing for Adhoc Networks
A-SAODV	–	Adaptive Secure AODV
ANN	–	Artificial Neural Network
CPDRT	–	Cutting Point of Disruption of Routing Table
CPDON	–	Cutting Point of Disruption of Originator Node
CPDRN	–	Cutting Point of Disruption of Relay Node
CDS-SAODV	–	Corrected Double Signature of Secure Adhoc On Demand Vector
CSS-SAODV	–	Corrected Single Signature of Secure Adhoc On Demand Vector
DRT	–	Disruption of Routing Table
DON	–	Disruption of Originator Node
DP-WHL	–	Diversion of Packet over Wormhole Link
DRN	–	Disruption of Relay Node
ESAODV	–	Extra Secure AODV
ECCDSA	–	Elliptic Curve Cryptography Digital Signature Algorithm
HBHA	–	Hybrid Blackhole Attack
IDS	–	Intrusion Detection System
IDSE	–	IDS Engine
JiST/SWANS	–	Java in Time Simulator/Scalable Wireless Adhoc Network Simulator
NRC	–	Non Repudiation Control
RREQ	–	Route Request
RREQSec	–	Route Request Secure
RREP	–	Route Reply
RREPSec	–	Route Reply Secure
RERR	–	Route Error

RERRSec	–	Route Error Secure
RSA	–	Rivest, Shamir and Adleman
SAODV	–	Secure AODV
SS-SAODV	–	Single Signature of SAODV
SPE	–	Secure Protocol Engine
ZDRT	–	Zero rates of DRT
ZDON	–	Zero rates of DON
ZDRN	–	Zero rates of DRN

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

In recent years, Mobile Adhoc Network (MANET) has been rapidly developed and has been used in many applications, ranging from military to civilian and commercial. The setting up of such network can be performed without either any human intervention or existence of infrastructure. Search and rescue missions, data collection, and virtual classrooms and conferences, are examples of applications for the network. Devices such as laptops, Personal Digital Assistants (PDAs), and smartphones are some of the MANET nodes that use wireless media in order to communicate among themselves.

MANET is more vulnerable than wired network because of its open medium. Figure 1.1 shows the susceptibility of benign nodes to attack conducted by attackers. In that figure, attackers can threaten and attack the benign nodes at any time from any node. Mobility, unavailability of a central administration in this network, and auto organizing capability among the nodes contribute to the network security holes. Moreover, the unique characteristics and constraints of the mobile nodes, which are incapable of generating their own power and limited power supply, also contribute to the network security risks.

The intrinsic vulnerabilities of mobile adhoc network lies within the wireless links, its routing protocols, and the auto-configuration mechanisms as detailed below.

a. Wireless links

   Wireless links make MANET susceptible to attack. It is easier for hackers to eavesdrop and gain access into the adhoc network for stealing the

Figure 1.1: MANET Susceptibility

confidential information. It is also easier for them to enter or leave the network because no physical connection is required. The attackers can also attack nodes for deleting messages, injecting false packets, or impersonating identities (Bellardo and Savage, 2003; Bicakci and Tavli, 2009). The final goal of the attack is to disrupt network service and to violate the network's goals, i.e., availability, integrity, authentication, and non-repudiation.

b. Routing protocols and end-to-end packets forwarding.
The routing protocols in MANET suffer from many attacks since their designs normally consider a trusted and collaborated environment (Yang *et al.*, 2004; Djenouri *et al.*, 2005). Their designs assume unavailability of attacks. However, in real scenario, attacks in the network are easily generated, and the types of attacks are many. For example, blackhole attack, by sending false routing information, implies bogus route entries in nodes routing tables. As a result, many incorrect routings exist, and cause bottleneck to the communication channels. In another case, an attacker can deceive security process by controlling traffic 'to' and 'from' entire parts of the network. In a worst case scenario, the malicious nodes can drop or modify the packets that travel through them.

c. Auto configuration.
As indicated by Buiati *et al.* (2004), and Wang *et al.* (2005), the auto-configuration brings up new functional vulnerabilities to false replies regardless of the protocols used. In this case, an attacker can utilize the information from the neighbors to deny a new host from joining the network. First, the attacker may verify all occupied addresses, thus claims the unoccupied addresses are in use. As a result a new host cannot join the network.

1.2 Research Motivations

The vulnerabilities of wireless link and auto configuration are native features of MANET that cannot be removed. However, the vulnerability of routing protocol can be managed or eliminated through security patches or security updates. Moreover, Caballero (2006) has proven that routing protocol is the most vulnerable point in the mobile adhoc network. As such many attacks are easily generated to cripple MANET operations.

Many works have been proposed to address the vulnerability of MANET through secure routing and packet forwarding. However, most of them only provide single security layer approach, i.e., either cryptographic authentication or intrusion detection system. In addition, their results have been also conducted without considering the extensive data analysis. Le Boudec (2010) stated that insufficient data analysis produces misinformative and incomprehensive results.

These problems motivate this research to explore and to provide better solutions than existing, which include both security solutions and performance analyses. Thus, the security solutions will deal with development of layered security concept as a framework for securing MANET routing. The framework consist of two security layers, i.e., a secure protocol in first layer, and intrusion detection with countermeasures in second layer. This concept resembles and adapts the security concept in the wired network, which is well known as a defense-in-depth architecture (Santos, 2007). Furthermore, the performance analyses present the models of the network performance measures that can also be applied as a general network performance measure.

1.3 Background of the Problem

This section presents a discussion on the limitations of exiting MANET routing protocols and the weakness of the proposed securities solutions. Last but not least, it discusses the limitation of performance analysis on the existing proposed security for MANET.

1.3.1 Limitations of MANET Routing Protocols

The early studies on MANET were focused on some fundamental problems of MANET routing protocols. The design of efficient routing protocols and new mobility models received many attentions from researchers. During the development, most researchers assumed that the protocols run in a trusted environment (Yang *et al.*, 2004; Djenouri *et al.*, 2005).

Routing protocol are normally categorized into three gorups. They are proactive, reactive, and hybrid routing protocols (Changling Liu, 2003; Abusalah *et al.*, 2008; Arora *et al.*, 2010). Djenouri *et al.* (2005) stated that the reactive protocols are more adaptable to MANET environment than the proactive. Bai and Singhal (2006) showed the reactive outperforms the proactive in terms of the packet delivery ratio, overhead and energy efficiency. Meanwhile, Junhai *et al.* (2009) concluded that the reactive is more scalable than the proactive routing protocol, although their source nodes might suffer from long delays of route searching. The hybrid adopts both features of proactive and reactive techniques in determining efficient routes. However, the hybrid routing protocol receives little attentions from MANET community since it needs more resources, such as computation and memory.

Several popular reactive routing protocols are Adhoc on Demand Vector (AODV) (Perkins and Royer, 1999; Perkins *et al.*, 2003) and Dynamic Source Routing (DSR)(Johnson, 1996; Johnson *et al.*, 2007). The protocols perform better operation than Destination Sequence Distance Vector (DSDV)(Perkins and Bhagwat, 1994) and Temporally Ordered Routing Algorithm (TORA)(Park and Corson, 2001) in several situations such as high density, high mobility, and high traffic (Feeney, 1999). All of these protocols do not consider any security measure (Djenouri *et al.*, 2005).

AODV suffers from falsification of both destination sequence number (DSN) and hop count fields (Djenouri *et al.*, 2005). This protocol is also susceptible to tunneling, spoofing, falsifying a route error and rushing attacks. Jiejun Kong (2003) showed that AODV is more vulnerable than anonymous on-demand routing protocol (ANODR). Weerasinghe and Fu (2008) demonstrated that AODV greatly suffers from cooperative blackhole attack. Through simulation, Arora *et al.* (2010), concluded that the AODV is also vulnerable to wormhole attack compared to DSR.

1.3.2 Limitations of the Existing Security Frameworks against the Attacks

Zhang and Lee (2005), and Wu *et al.* (2007) differentiated attacks in MANET routing into simple and sophisticated attacks. Based on the simplicity in triggering the attacks, blackhole attack (Deng *et al.*, 2002; Sun *et al.*, 2003a) is the most dangerous attack in the type of simple attacks. Meanwhile, wormhole attack (Hu *et al.*, 2003a, 2006) is the most severe attack in the type of sophisticated attacks. Therefore, many efforts have been devoted to address both types of attacks. In general, the defense from those attacks can be categorized into preventive and reactive techniques (Wu *et al.*, 2007; Lima *et al.*, 2009).

The preventive technique adopts cryptography as the basis of defense to those attacks. The technique often employs symmetric key, digital public key and digital certificate for authenticating and for maintaining the integrity of routing packets. Some researchers, e.g. Smith *et al.* (1997); Jacobs and Corson (1999); Binkley and Trost (2001); Zapata and Asokan (2002); Sanzgiri *et al.* (2002, 2005); Papadimitratos and Haas (2002), and Hu and Perrig (2005), use the technique in their works. Unfortunately, these works are conducted without considering extensive test based on attacks. Therefore, the strength of the cryptography to the attacks cannot be demonstrated.

To overcome the limitations on the security testing, several researchers consider a well-known attack, blackhole attack, in their proposed security. Ramaswami and Upadhyaya (2006) implemented this attack for evaluating a modified Secure AdHoc on-Demand Vector (SAODV). They also introduced ACK packet that is modified from a route reply (RREP) packet. However, ACK

packet has a different of routing path compared to the RREP. The goal of the modification is to improve the security strength of SAODV. Unfortunately, this modification decreases the number of delivered packets and degrades the network performance compared to the original SAODV.

Other researchers, Lu *et al.* (2009), proposed Secure AODV (SAODV). It should be noted that the name of their proposed scheme is similar to Zapata and Asokan's scheme but no correlation between the twos schemes. The authors also implement blackhole attack in evaluating the proposed security. This attack is generated by a node that has been setup as attacker or Bad Adhoc On-demand Distance Vector (BAODV). Thus, based on testing results, the authors developed a mechanism for defending MANET routing from this attack. Unfortunately, the results show that the SAODV (Lu *et al.*, 2009) consumes extra memory and CPU resources.

All proposed secure protocols as described so far also suffer from factorization attack (crypto attack). The digital signatures or certificates, used by the secure protocols, are tractable in the quantum computer. Shor (1997) has proven that factoring the digital signatures are simple. Moreover, Roblot (2004); ChÃĺze and Galligo (2006); Wallace and White (2008) and Zhai (2009) strengthen Shor's results.

The reactive technique keeps track or monitors to their neighbor activities for determining whether suspicious activities occur. The technique is well known as intrusion detection. In real world, the technique is realized as an intrusion detection system (IDS). There are three groups of IDS based on the mechanism of detection (Mishra *et al.*, 2004). They are signature based IDS, anomaly based IDS, and specification based IDS (a hybrid both signature and anomaly based IDS). The signature based IDS compares incoming packets with pre-known attacks (or signature of attack). The anomaly based IDS attempts to detect activities that differ from the normal expected system behavior. Meanwhile, the specification based IDS performs monitoring on operation of a system using security specification (security rule).

Several IDSes have been directed to detect simple attacks in MANET. Kurosawa *et al.* (2007); Cheng *et al.* (2008); Fourati *et al.* (2008); Roy *et al.* (2010), and Su (2011) proposed IDS for detecting blackhole attack. Bononi and Tacconi (2007) use a combination of 'intrusion detection and cryptography' for detecting

several attacks (blackhole, route disruption, and DOS attacks). Meanwhile, Lauf *et al.* (2010) proposed IDS for identifying spoofing attacks in MANET. These IDSes consider the anomaly detection. In fact, anomaly detection needs large memory, requires much CPU resources and slow in detecting attacks. Indeed, since the goal of these IDSes is to detect simple attacks, they are incapable of identifying sophisticated attacks such as the wormhole attack.

Some researchers, such as Hu *et al.* (2003a, 2006), Poovendran and Lazos (2007), Qian *et al.* (2007), Vu *et al.* (2008), Nait-Abdesselam (2008), and Su (2010) proposed mechanisms to defend MANET from wormhole attack. However, Hu *et al.* (2003a, 2006) technique needs extra hardware, i.e., Global Positioning System (GPS)-disciplined clock for time synchronization. Poovendran and Lazos's technique incurs huge computation resources since they adopt graph theory in detecting the wormhole attack. Intrusion detection based on statistical analysis of multi-path (SAM) (Qian *et al.*, 2007) considers anomaly as the mechanism of detection. As such SAM is slow in detecting wormhole attack and needs huge data for learning a normal behavior. A security solution for the wormhole by Nait-Abdesselam (2008) is inaccurate to detect wormhole attack in a high density of adhoc network. Moreover, Wormhole Avoidance Routing Protocol (WARP) (Su, 2010) suffers in performance because it removes the capability of answering route request packets in the middle nodes even though the nodes have the requested route.

Figure 1.2 summarizes the security problems and the existing works to secure the network. Referring to the figure, routing protocols of the network suffer from spoofing, blackhole, and wormhole attacks. The attacks disrupt MANET's routing, determine inaccurate interpretation of the network topology, and contribute to the abnormality of packet's delivery. In the worst case, the attacks cause congestion within the network and increase the possibility of confidential data theft. In short, most of the existing protections for MANET are insufficient to defend the network from both simple and sophisticated attacks. They have a limitation to the effect of prevention techniques in general since most of them consider only single security layer in the network. It is incomprehensive in term of security mechanism since attackers can directly strike to the target after they succeeded in breaking the single security layer.

In addition to the limitation of the existing works for securing MANET is the performance due to security implementation. Most of the existing protections

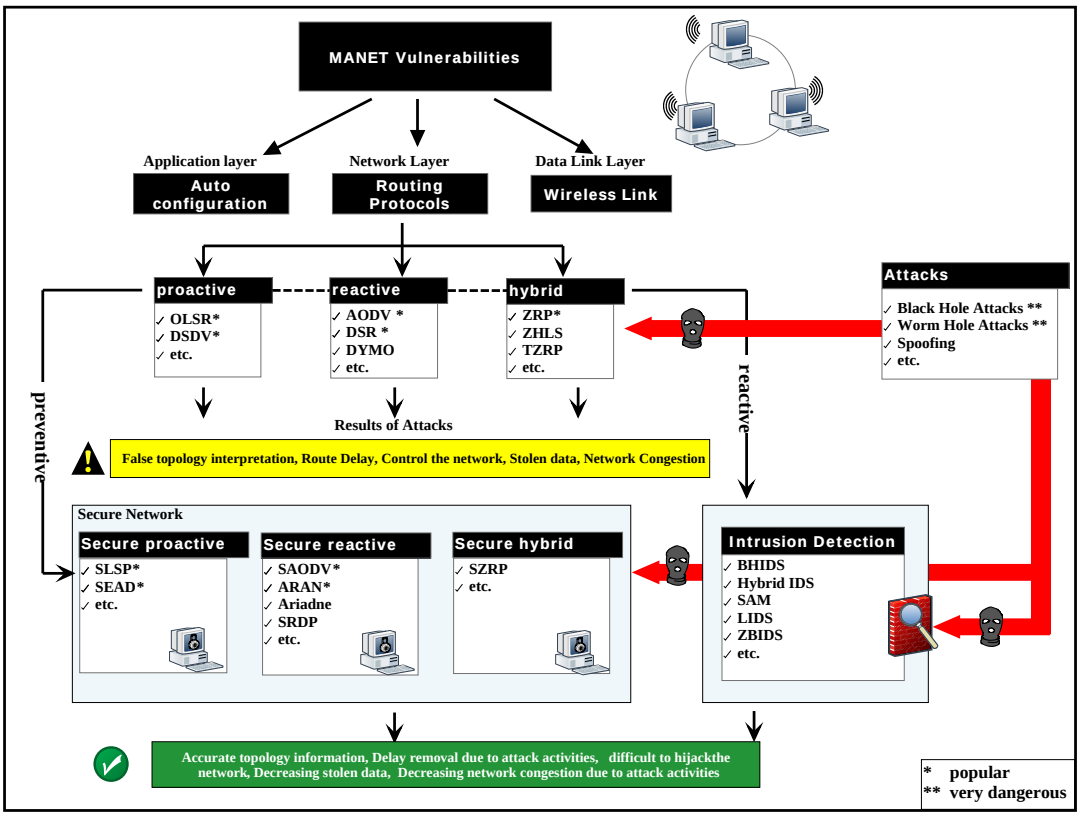

Figure 1.2: Illustration of the problems background

need much resources, e.g., memory and CPU, and slow in detecting both types of attacks. It is contradictory to the natures of mobile adhoc network, which have limited power supply, memory and CPU resources. Furthermore, the existing protections based on authentication also suffer from factorization attacks, and some of the proposed defenses from wormhole attack require extra hardware.

1.3.3 Limitations of Performance Analysis on the Existing Proposed Security for MANET

There are two ways in performing performance analysis in MANET, i.e., 'analytical of performance based on purely mathematical science' and 'simulation of performance based on discrete event simulation (DES)' (see Bolch *et al.* (2006) for details). Analytical approach observes and uses many assumptions on the network parameters and the network variables in achieving tractable network models (Hanbali *et al.*, 2008). Through the models, this approach describes the network performance as reported by Groenevelt *et al.* (2005), Zhang *et al.* (2007), and Hanbali *et al.* (2008). In contrast, the simulation based on DES

relies on a simulator software to demonstrate the network performance, such as in Gnana Durai and Parthasarathy (2005); Razak *et al.* (2008), and Komninos and Douligeris (2009).

The network parameters and variables increase proportionally with the complexity of the network. Simplifying the parameters and variables can reduce the reliability of the network models. Meanwhile, the development of models that consider many network parameters and variables are complicated. For an example, the reliability of route in MANET is often impossible to be simplified and to be modeled due its NP-complete problems (Ghalavand *et al.*, 2010). Therefore, simplifying parameters such in analytical approaches are unreliable methods for describing the network performance. In this situation, DES can be used to demonstrate the network performance. However, it needs extensive analysis on the data of experiments.

Most of MANET performance analyses based on simulation do not provide extensive analysis on the experimental results. Gnana Durai and Parthasarathy (2005); Ramaswami and Upadhyaya (2006); Razak *et al.* (2008); Komninos and Douligeris (2009), and Lu *et al.* (2009) perform simple analysis based on raw data from simulators in their reports. They present the results of performance in simple graphs based on the data, and disregards mathematical models. As such, their works are insufficient to predict the future outcomes without rerunning the simulation in the new configuration. In addition, the results are also incapable in describing which potential source has contributed to the results.

1.4 Research Questions

As indicated in Section 1.2, this research proposes a new framework for securing MANET from the attacks, and provides extensive analyses of the security framework performance. Thus, it is a challenge to develop the security framework and to provide MANET performance analysis based on the experimental data. The following is the list of research questions for achieving the goals of this research.

a. On measuring the vulnerability of existing MANET routing protocol to existing and future types of attacks, the following research questions are answered:

   (i) How to objectively measure the vulnerability of MANET routing protocol?

   (ii) What are the possible future attacks for MANET and how to measure the severity of the attacks?

   (iii) How to represent the attacks in the simulation test-bed?

b. On designing, improving and analyzing a new lightweight layered security framework to counter simple attack that is represented by blackhole attack, the following research questions are answered:

   (i) What are the components of the new security framework that counter the above attack?

   (ii) How to maintain integrity, prevent from deceiving activities and provide immune from factorization attack?

   (iii) How to design a light weight framework that require smaller packet size and less computation resources?

c. On designing, improving and analyzing the enhancement of the security framework to counter sophisticated attack that is represented by wormhole attack, the following research questions are answered:

   (i) What are the components of the enhancement of the security framework that counter wormhole attack?

   (ii) How to design the detection algorithms for detecting the attack in near realtime?

   (iii) How to design the countermeasures that can react efficiently on the attacks detected?

   (iv) How to design an efficient spreading red messages to warn the network under attack?

d. On proposing and analyzing the performance of the security framework based on regression and neural network data analysis, the following research questions are answered:

(i) How to design the models of the security framework performance based on experimental data?

(ii) Why the model considers more than one techniques to profile the security framework performance?

From those points above, the following is the main research question to be answered: ***"How to develop a robust security mechanism to protect AODV routing protocol?"***

1.5 Research Objectives

There are four research objectives of this research:

(a) To objectively measure the vulnerability of existing MANET routing protocol to existing and future types of attacks.

(b) To design, improve and analyze a new lightweight layered security framework to counter simple attack that is represented by blackhole attack.

(c) To design, improve and analyze the enhancement of the security framework to counter sophisticated attack that is represented by wormhole attack.

(d) To propose and analyze the performance of the security framework based on regression and neural network data analysis.

1.6 Scopes

Some scopes are applied to this research work in order to keep the observation tractable. They are:

(a) This research enhances AODV routing protocol security as it is the most widely used protocol for MANET.

(b) This research focuses on the security of network layer, and assume that all benign nodes consider all security protections when the network under attacks (blackhole and wormhole attacks)

(c) This research considers using ideal data link communication of MANET.

(d) All nodes participants implements conventional IPv4 addressing model.

(e) For analysis based on regression, this research assumes that each of the performance metrics (response) is independent of each others; it means that there is no relationship between the performance metrics.

1.7 Research Contributions

This work has primary research contributions and secondary research contributions. The following is the primary research contributions.

(a) A new MANET security metrics for the measurement of the severity of attacks.

(b) A new efficient secure protocol that is immune from factorization attack.

(c) Novel algorithms of IDS to detect both simple and sophisticated attacks.

(d) The network performance models based on regression and neural network data analysis for profiling the security of MANET routing protocols.

The secure protocol and IDS with countermeasures complements each other for preventing MANET from the attacks. They are bounded within new security framework for securing the network. In addition, the proposed securities do not add the complexity of the network. Thus, the secondary research contribution is as below:

(a) New variants of blackhole and wormhole attacks to represent possible future class of attacks.

(b) Corrected SAODV architecture.

(c) Enhanced Java in Time Simulator/Scalable Wireless Adhoc Network Simulator (JiST/SWANS) (http://jist.ece.cornell.edu/, 2010) as a MANET security simulator.

1.8 Outline of Thesis

This work studied three important topics in MANET: secure routing protocol, intrusion detection with countermeasure and performance metrics models. The chapter of this thesis is organized as follows.

Chapter 1, Introduction. Chapter 1 discusses overview, motivations, background of problems, research question, and contributions of this research.

Chapter 2, Literature Review. Chapter 2 discusses and reviews the current research works in securing MANET routing.

Chapter 3, Research Methodology. Chapter 3 discusses the research methodology adopted in designing security and in modeling performance of the MANET routing protocol.

Chapter 4, Enhanced Security for MANET Routing Protocol. Chapter 4 implements the research framework in order to design and develop enhanced security for AODV routing protocol.

Chapter 5, Modeling Data of Performance. Chapter 5 analyzes the data of ESAODV to develop the performance of the layered security of MANET routing.

Chapter 6, Summary and Future Works. Chapter 6 summarizes and discusses some specific topics for future works.

REFERENCES

Aad, I., Hubaux, J.-P. and Knightly, E. W. (2004). Denial of service resilience in ad hoc networks. In *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*. September 26 - October 01. New York, NY, USA: ACM. ISBN 1-58113-868-7, 202–215. doi:http://doi.acm.org/10.1145/1023720.1023741.

Aad, I., Hubaux, J.-P. and Knightly, E. W. (2008). Impact of Denial of Service Attacks on Ad Hoc Networks. *IEEE/ACM TRANSACTIONS ON NETWORKING*. 16(4), 791–802. doi:10.1109/TNET.2007.904002.

Abusalah, L., Khokhar, A. and Guizani, M. (2008). A survey of secure mobile Ad Hoc routing protocols. *IEEE Communications Surveys & Tutorials*. 10(4), 78–93. doi:10.1109/SURV.2008.080407.

Acs, G. (2009). *Secure Routing In Multi-hop Wireless Networks*. Ph.D. Thesis. Budapest University of Technology And Economics.

Adjih, C., Clausen, T., Jacquet, P., Laouti, A., M., P. and Raffo, D. (2003). Securing the OLSR protocol. In *Proceedings of Med-Hoc-Net*. June. Mahdia, Tunisia, 25–27.

Aiello, W., Lodha, S. and Ostrovsky, R. (1998). *Fast digital identity revocation*, Springer Berlin / Heidelberg, vol. 1462. 137–152–152.

Albers, P., Camp, O., marc Percher, J., Jouga, B. and Puttini, R. (2002). Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches. In *Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002)*. April. 1–12.

Andel, T. and Yasinsac, A. (2007). The invisible node attack revisited. In *SoutheastCon, 2007. Proceedings. IEEE*. 686 –691. doi:10.1109/SECON.2007.342988.

Anderson, J. P. (1980). *Computer security threat monitoring and surveillance*. Technical report. Fort Washington, PA: James P. Anderson Co.

Apache Software Foundation, L. (2010). *log4j - Logging Services*. Internet. Retrievable at http://logging.apache.org/log4j/1.2/.

Arora, M., Challa, R. and Bansal, D. (2010). Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks. In *Computer and Network Technology (ICCNT), 2010 Second International Conference on*. April. 102 –104. doi:10.1109/ICCNT.2010.34.

Bai, R. and Singhal, M. (2006). DOA: DSR over AODV Routing for Mobile Ad Hoc Networks. *Mobile Computing, IEEE Transactions on*. 5(10), 1403 –1416. ISSN 1536-1233. doi:10.1109/TMC.2006.150.

Baras, J. S., Radosavac, S., Theodorakopoulos, G., Sterne, D., Budulas, P. and Gopaul, R. (2007). Intrusion Detection System Resiliency to Byzantine Attacks: The Case Study of Wormholes in OLSR. In *Military Communications Conference, 2007. MILCOM 2007. IEEE*. 1 –7. doi:10.1109/MILCOM.2007.4455008.

Barbeau, M. and Kranakis, E. (2007). *Principles of Ad Hoc Networking*. ISBN: 978-0-470-03290-9. The Atrium, Southern Gate, Chichester - West Sussex PO19 8SQ, England: John Wiley & Sons, Ltd.

Barr, R., Haas, Z. J. and van Renesse, R. (2005). JiST: an efficient approach to simulation using virtual machines: Research Articles. *Softw. Pract. Exper.* 35, 539–576. ISSN 0038-0644. doi:10.1002/spe.v35:6. Retrievable at http://portal.acm.org/citation.cfm?id=1060168.1060170.

Bellardo, J. and Savage, S. (2003). 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In *the Proceedings of 12th USENIX Security Symposium*. August. 15–28.

Bellur, B. and Ogier, R. (1999). A reliable, efficient topology broadcast protocol for dynamic networks. vol. 1. mar. 178 –186 vol.1. doi:10.1109/INFCOM.1999.749266.

Bennett, C. H., Bernstein, E., Brassard, G. and Vazirani, U. (1997). Strengths and Weaknesses of Quantum Computing. *SIAM Journal on Computing*. 26(5), 1510–1523. doi:10.1137/S0097539796300933. Retrievable at http://link.aip.org/link/?SMJ/26/1510/1.

Bettstetter, C., Resta, G. and Santi, P. (2003). The node distribution of the random waypoint mobility model for wireless ad hoc networks. *Mobile Computing, IEEE Transactions on*. 2(3), 257 – 269. ISSN 1536-1233. doi:10.1109/TMC.2003.1233531.

Bicakci, K. and Tavli, B. (2009). Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards & Interfaces*. 31(5), 931 – 941. ISSN 0920-5489. doi:DOI:10.1016/j.

csi.2008.09.038. Retrievable at http://www.sciencedirect.com/science/article/B6TYV-4TYYT70-1/2/1a7949e3362b28628f5ba216c1306f83, specification, Standards and Information Management for Distributed Systems.

Binkley, J. and Trost, W. (2001). Authenticated ad hoc routing at the link layer for mobile systems. *Wireless Networks*. 7(2), 139–145. Kluwer Academic Publishers.

Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer Science Business Media, LLC.

Blazevic, L., Buttyan, L., Capkun, S., Giordano, S., Hubaux, J.-P. and Le Boudec, J.-Y. (2001). Self organization in mobile ad hoc networks: the approach of Terminodes. *Communications Magazine, IEEE*. 39(6), 166 –174. ISSN 0163-6804. doi:10.1109/35.925685.

Bolch, G., Greiner, S., de Meer, H. and Trivedi, K. S. (2006). *Queueing Networks and Markov Chains, Modeling and Performance Evaluation with Computer Science Applications*. (2nd ed.). John Wiley & Sons, Inc.

Bononi, L. and Tacconi, C. (2007). Intrusion detection for secure clustering and routing in Mobile Multi-hop Wireless Networks. *International Journal of Information Security*. 6, 379–392. ISSN 1615-5262. Retrievable at http://dx.doi.org/10.1007/s10207-007-0035-9.

Bragg, R. (2003). *CISSP Training Guide*. Que Publishing.

Brutch, P. and Ko, C. (2003). Challenges in intrusion detection for wireless ad-hoc networks. In *Proceedings of the Applications and the Internet Workshops*. Jan. 368–373.

Buchegger, S. and Boudec, J. Y. L. (2002). Performance Analysis of the Confidant protocol. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc networking and Computing*. June. 226–236. Retrievable at http://doi.acm.org/10.1145/513800.513828.

Buchmann, J., Dahmen, E., Klintsevich, E., Okeya, K. and Vuillaume, C. (2007). Merkle Signatures with Virtually Unlimited Signature Capacity. In Katz, J. and Yung, M. (Eds.) *Applied Cryptography and Network Security*. (pp. 31–45). *Lecture Notes in Computer Science*, vol. 4521. Springer Berlin / Heidelberg. Retrievable at http://dx.doi.org/10.1007/978-3-540-72738-5_3.

Buchmann, J., GarcÃ■a, L., Dahmen, E., DÃűring, M. and Klintsevich, E. (2006). CMSS - An Improved Merkle Signature Scheme. In Barua, R. and Lange, T. (Eds.) *Progress in Cryptology - INDOCRYPT 2006*. (pp. 349–363). *Lecture Notes in Computer Science*, vol. 4329. Springer Berlin / Heidelberg.

Retrievable at http://dx.doi.org/10.1007/11941378_25.

Buiati, F., Puttini, R., de Sousa, R., Abbas, C. B. and Villalba, L. G. (2004). Authentication and Autoconfiguration for MANET Nodes. In Yang, L. T., Guo, M., Gao, G. R. and Jha, N. K. (Eds.) *Embedded and Ubiquitous Computing*. (pp. 64–66). *Lecture Notes in Computer Science*, vol. 3207. Springer Berlin / Heidelberg. Retrievable at http://dx.doi.org/10.1007/978-3-540-30121-9_5.

Caballero, E. J. (2006). Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem. In *Security and Privacy in Pervasive Computing - TKK T-110.5290 Seminar on Network Security, Autumn 2006*. ISBN: 978-951-22-8595-2. http://www.tml.hut.fi/Publications/C/22/.

Capkun, S., ButtyÃąn, L. and Hubaux, J.-P. (2003). SECTOR: secure tracking of node encounters in multi-hop wireless networks. In *In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN*. 21–32.

Carter, E. and Hogue, J. (2006). *Intrusion Prevention Fundamentals*. Cisco Press.

Castelluccia, C., Saxena, N. and Yi, J. H. (2005). Self-configurable key pre-distribution in mobile ad hoc networks. In *in: IFIP Networking Conference*. 1083–1095.

Cerri, D. and Ghioni, A. (2008). Securing AODV: the A-SAODV secure routing prototype. *IEEE Communications Magazine*. 46(2), 120–125. doi:10.1109/MCOM.2008.4473093.

Chakeres, I. and Perkins, C. (2008). *Dynamic MANET on demand Routing Protocol*. INTERNET-DRAFT (draft-ietf-manet-dymo-12.txt). Retrievable at http://ianchak.com/dymo/draft-ietf-manet-dymo-12.txt.

Chan, E., Chan, H., Chan, K., Chan, V., Chanson, S., Cheung, M., Chong, C., Chow, K., Hui, A., Hui, L., Lam, L., Lau, W., Pun, K., Tsang, A., Tsang, W., Tso, S., Yeung, D.-Y. and Yu, K. (2004). IDR: an intrusion detection router for defending against distributed denial-of-service (DDoS) attacks. In *Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks*. May. ISSN 1087-4089, 581–586. doi:10.1109/ISPAN.2004.1300541.

Changling Liu, J. K. (2003). *A Survey of Mobile Ad Hoc network Routing Protocols*. Technical report. Department of Computer Structures - University of Ulm - Germany: University of Ulm.

Chen, L., Leneutre, J. and Puig, J.-J. (2006). A Secure and Efficient Link State Routing Protocol for Ad Hoc Networks. In *Wireless and Mobile Communications, 2006. ICWMC '06. International Conference on*. July. 36

–36. doi:10.1109/ICWMC.2006.14.

Cheng, B., Chen, H., Tseng, R. and Nov, D.-. (2008). A Good IDS Response Protocol of MANET Containment Strategies. *Ieice T Commun Ieice T Commun Ieice Transactions on Communications*. E91b(11), 3657–3666.

Cherkassky, V. and Mulier, F. (2007). *Learning from Data Concepts, Theory, and Methods*. (2nd ed.). IEEE Press - A John Wiley & Sons, Inc.

Chiang, C.-C., Wu, H.-K., Liu, W. and Gerla, M. (1997). Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. In *IEEE Singapore International Conference on Networks, SICON'97, April 16-17, 1997, Singapore*. April. IEEE, IEEE, 197–211. Retrievable at http://www.ics.uci.edu/~atm/adhoc/paper-collection/gerla-routing-clustered-sicon97.pdf.

Chiu, H. and Wong Lui, K. (2006). DelPHI: wormhole detection mechanism for ad hoc wireless networks. In *The 1st International Sysmposium on Wireless Pervasive Computing*. 10.1109/ISWPC.2006.1613586. Retrievable at http://hdl.handle.net/10722/45913.

ChÃĺze, G. and Galligo, A. (2006). From an approximate to an exact absolute polynomial factorization. *Journal of Symbolic Computation*. 41(6), 682 – 696. ISSN 0747-7171. doi:DOI:10.1016/j.jsc.2005.11.004. Retrievable at http://www.sciencedirect.com/science/article/B6WM7-4J32JDX-1/2/2c721593ed4b3c873a6a242c25f8268b.

Clausen, T. and Jacquet, P. (2003). *Optimized Link State Routing Protocol (OLSR)*. Internet draft 3626 (rfc3626.txt). Retrievable at http://www.ietf.org/rfc/rfc3626.txt.

Currell, G. and Dowman, A. (2009). *Essential Mathematics and Statistics for Science Second Edition*. A John Wiley & Sons, Ltd.

Dahmen, E. (2009). *Post-quantum signatures for today*. Ph.D. Thesis. Technischen UniversitÂĺat Darmstadt genehmigte.

Darmstadt, T. U. (2010). *The FlexiProvider*. Retrievable at http://www.flexiprovider.de, accessed on Oct 2010.

Deng, H., Li, W. and Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications Magazine*. 40(10), 70–75. doi:10.1109/MCOM.2002.1039859.

Denning, D. (1987). An Intrusion-Detection Model. *Software Engineering, IEEE Transactions on*. SE-13(2), 222–232. ISSN 0098-5589.

Diffie, W. and Hellman, M. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on*. 22(6), 644 – 654. ISSN 0018-9448. doi:10.1109/TIT.1976.1055638.

Djenouri, D., Khelladi, L. and Badache, A. N. (2005). A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications Surveys & Tutorials*. 7(4), 2–28. doi:10.1109/COMST.2005.1593277.

Dong, D., Li, M., Liu, Y., Li, X.-Y. and Liao, X. (2009a). Topological detection on wormholes in wireless ad hoc and sensor networks. In *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*. ISSN 1092-1648, 314 –323. doi:10.1109/ICNP.2009.5339673.

Dong, Y., Chim, T. W., Li, V. O., Yiu, S. and Hui, C. (2009b). ARMR: Anonymous routing protocol with multiple routes for communications in mobile ad hoc networks. *Ad Hoc Networks*. 7(8), 1536 – 1550. ISSN 1570-8705. doi:DOI:10.1016/j.adhoc.2009.04.010. Retrievable at http://www.sciencedirect.com/science/article/B7576-4W4JDSN-1/2/771d6d33da7d945c864a1601026c5a75, privacy and Security in Wireless Sensor and Ad Hoc Networks.

Dong, Y., Sui, A.-F., Yiu, S., Li, V. O. and Hui, L. C. (2007). Providing distributed certificate authority service in cluster-based mobile ad hoc networks. *Computer Communications*. 30(11-12), 2442 – 2452. ISSN 0140-3664. doi:DOI:10.1016/j.comcom.2007.04.011. Retrievable at http://www.sciencedirect.com/science/article/B6TYP-4NMC89M-1/2/6315e5e8e907baf77bb11270787c5816, special issue on security on wireless ad hoc and sensor networks.

Douceur, J. R. (2002). The Sybil Attack. In Druschel, P., Kaashoek, F. and Rowstron, A. (Eds.) *Peer-to-Peer Systems (Lecture Notes in Computer Science Volume 2429)*. (pp. 251–260). vol. 2429/2002. Springer-Verlag Berlin Heidelberg NewYork: Springer Berlin / Heidelberg.

Drapper, N. and Smith, H. (1998). *Applied Regression Analysis 3rd Ed.* John Wiley & Sons, Inc.

Dube, R., Rais, C., Wang, K.-Y. and Tripathi, S. (1997). Signal stability-based adaptive routing (SSA) for ad hoc mobile networks. *Personal Communications, IEEE*. 4(1), 36 –45. ISSN 1070-9916. doi:10.1109/98.575990.

Endorf, C., Schultz, G. and Mellander, J. (2004). *Intrusion Detection & Prevention*. Brandon A. Nordin.

Engelbrecht, A. P. (2007). *Computational Intelligence, An Introduction*. (2nd ed.). ISBN:978-0-470-03561-0. John Wiley & Sons Ltd. Retrievable at www.wiley.com.

Faraway, J. J. (2005). *Linear Models with R*. Chapman & Hall/CRC. Retrievable at www.crcpress.com.

Feeney, L. M. (1999). *A Taxonomy for Routing Protocols in Mobile Ad Hoc Networks*. Technical report. Box 1263, SE-164 29 Kista, Sweden: Swedish Institute of Computer Science.

Fourati, A., Al Agha, K. and Dec, D.-. (2008). Detecting forged routing messages in ad hoc networks. *Telecommun Syst Telecommun Syst Telecommunication Systems*. 39(3-4), 205–214 ST – Detect. 379RA Times Cited:0 Cited References Count:14.

Galmacci, G. (1996). Collinearity detection in linear regression models. *Computational Economics*. 9, 215–227. ISSN 0927-7099. Retrievable at http://dx.doi.org/10.1007/BF00121635.

Garcia-Luna-Aceves, J. J. (2002). Flow-oriented protocols for scalable wireless networks. In *MSWiM '02: Proceedings of the 5th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems*. New York, NY, USA: ACM. ISBN 1-58113-610-2, 1–6. doi:http://doi.acm.org/10.1145/570758.570759.

Garcia-Luna-Aceves, J. J. and Spohn, M. (1999). Source-Tree Routing in Wireless Networks. In *Proceedings of the 7th International Conference on Network Protocols (IEEE ICNP 99), October 1999, Toronto, Candada*. October. IEEE, 273–282.

Garetto, M. and Leonardi, E. (2007). Analysis of Random Mobility Models with Partial Differential Equations. *Mobile Computing, IEEE Transactions on*. 6(11), 1204 –1217. ISSN 1536-1233. doi:10.1109/TMC.2007.1023.

Ghalavand, G., Dana, A., Ghalavand, A. and Rezahosieni, M. (2010). Reliable routing algorithm based on fuzzy logic for Mobile Ad Hoc Network. In *Proc. 3rd Int Advanced Computer Theory and Engineering (ICACTE) Conf*, vol. 5. doi:10.1109/ICACTE.2010.5579341.

Gnana Durai, P. and Parthasarathy, R. (2005). Self-organized Security Architecture for MANET. In Das, G. and Gulati, V. (Eds.) *Intelligent Information Technology*. (pp. 169–179). *Lecture Notes in Computer Science*, vol. 3356. Springer Berlin / Heidelberg. Retrievable at http://dx.doi.org/10.1007/978-3-540-30561-3_18.

Goetz, B., Peierls, T., Bloch, J., Bowbeer, J., Holmes, D. and Lea, D. (2006). *Java Concurrency in Practice*. ISBN-10: 0-321-34960-1. Addison Wesley Professional.

Groenevelt, R., Nain, P. and Koole, G. (2005). The message delay in mobile ad hoc networks. *Performance Evaluation*. 62(1-4), 210 – 228. ISSN 0166-5316. doi:DOI:10.1016/j.peva.2005.07.018. Retrievable at http://www.sciencedirect.com/science/article/B6V13-4GWBDNX-1/2/e649f31bf9844b2a5d949445d9e0e2be, performance 2005.

Grossglauser, M. and Tse, D. (2002). Mobility increases the capacity of ad hoc wireless networks. *Networking, IEEE/ACM Transactions on*. 10(4), 477 – 486. ISSN 1063-6692. doi:10.1109/TNET.2002.801403.

Gunther, F. and Fritsch, S. (2010). neuralnet: Training of Neural Networks. *The R Journal*. 2, 30–37.

GutiÃl'rrez, R., del Pozo, F. and Boccaletti, S. (2011). Node Vulnerability under Finite Perturbations in Complex Networks. *PLoS ONE*. 6(6), e20236. doi:10.1371/journal.pone.0020236. Retrievable at http://dx.doi.org/10.1371%2Fjournal.pone.0020236.

Haas, Z. and Barr, R. (2005). Density-independent, scalable search in ad hoc networks. In *Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on*, vol. 2. September. 1401 –1408 Vol. 2. doi:10.1109/PIMRC.2005.1651669.

Haas, Z. and Pearlman, M. (2001). The performance of query control schemes for the zone routing protocol. *Networking, IEEE/ACM Transactions on Networking, IEEE/ACM Transactions on*. 9(4), 427–438.

Haas, Z. J., Pearlman, M. R. and Samar, P. (2002). *The Zone Routing Protocol (ZRP) for Ad Hoc Networks*. Internet draft (draft-ietf-manet-zone-zrp-04.txt). Retrievable at http://www.ietf.org/proceedings/55/I-D/draft-ietf-manet-zone-zrp-04.txt, expires January 2003.

Hafslund, A., TÃÿnnesen, A., Rotvik, R. B., Andersson, J. and ÃŸivind Kure (2004). Secure Extension to the OLSR protocol. In *OLSR Interop and Workshop*. August. 1–4.

Haller, N. and Bellcore (1995). *RFC 1760 - The S/KEY One-Time Password System*. Request for Comments 1760 (rfc1760.html). Retrievable at http://www.faqs.org/rfcs/rfc1760.html.

Hallgren, S. and Vollmer, U. (2009). Quantum computing. In Bernstein, D. J., Buchmann, J. and Dahmen, E. (Eds.) *Post-Quantum Cryptography*. (pp. 15–34). Springer Berlin Heidelberg. ISBN 978-3-540-88702-7. Retrievable at http://dx.doi.org/10.1007/978-3-540-88702-7_2.

Hamma, T., Katoh, T., Bista, B. B. and Takata, T. (2006). An Efficient ZHLS Routing Protocol for Mobile Ad Hoc Networks. In *Proc. 17th Int. Workshop Database and Expert Systems Applications DEXA '06*. 66–70. doi:10.1109/DEXA.2006.24.

Hanbali, A. A., Nain, P. and Altman, E. (2008). Performance of ad hoc networks with two-hop relay routing and limited packet lifetime (extended version). *Performance Evaluation*. 65(6-7), 463 – 483. ISSN 0166-5316. doi:DOI:10.1016/j.peva.2007.12.005. Retrievable at http://www.sciencedirect.com/science/article/B6V13-4RFSCRB-1/2/05051b09a3fbeadc6496a2d38bd7bea6, innovative Performance Evaluation Methodologies and Tools: Selected Papers from ValueTools 2006.

Haykin, S. (1999). *Neural Network - A Comprehensive Foundation*. (2nd ed.). Prentice-Hall, Inc.

Heberlein, L., Dias, G., Levitt, K., Mukherjee, B., Wood, J. and Wolber, D. (1990). A network security monitor. In *Proceedings IEEE Computer Society Symposium on Research in Security and Privacy*. May. 296–304. doi:10.1109/RISP.1990.63859.

Hilewitz, Y., Yin, Y. and Lee, R. (2008). Accelerating the Whirlpool Hash Function Using Parallel Table Lookup and Fast Cyclical Permutation. In Nyberg, K. (Ed.) *Fast Software Encryption*. (pp. 173–188). *Lecture Notes in Computer Science*, vol. 5086. Springer Berlin Heidelberg. ISBN 978-3-540-71038-7.

Hornik, K., Stinchcombe, M. and White, H. (1989). Multilayer feedforward networks are universal approximators. *Neural Networks*. 2(5), 359 – 366. ISSN 0893-6080. doi:DOI:10.1016/0893-6080(89)90020-8. Retrievable at http://www.sciencedirect.com/science/article/B6T08-485RHTR-5R/2/5d13881c0b9d8128fde7950a6f55849d.

Hsu, C.-L. and Wu, T.-S. (2005). Self-certified threshold proxy signature schemes with message recovery, nonrepudiation, and traceability. *Applied Mathematics and Computation*. 164(1), 201 – 225. ISSN 0096-3003. doi:DOI:10.1016/j.amc.2004.04.097. Retrievable at http://www.sciencedirect.com/science/article/B6TY8-4DNRX0N-4/2/a185af52a003c5ca3e9d61e9211f4139.

http://jist.ece.cornell.edu/ (2010). *JiST / SWANS - Java in Simulation Time / Scalable Wireless Ad hoc Network Simulator*. Internet. Retrievable at http://www.r-project.org/.

Hu, L. and Evans, D. (2004). Using Directional Antennas to Prevent Wormhole Attacks. In *Network and Distributed System Security Symposium*. San Diego, 5-6 February 2004. Retrievable at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.135.7144.

Hu, Y. C. and Perrig, A. (2005). Ariadne: A Secure On-Demand Routing Protocols for Ad Hoc Networks. *Wireless Networks*. 11(1-2), 21–38.

Hu, Y.-C., Perrig, A. and Johnson, D. (2006). Wormhole attacks in wireless networks. *Selected Areas in Communications, IEEE Journal on*. 24(2), 370 – 380. ISSN 0733-8716.

Hu, Y.-C., Perrig, A. and Johnson, D. B. (2003a). Packet leashes: a defense against wormhole attacks in wireless networks. In *Proceedings of the INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3. April. 1976–1986.

Hu, Y.-C., Perrig, A. and Johnson, D. B. (2003b). Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of the 2nd ACM workshop on Wireless security*. San Diego, CA, USA: ACM, New York, NY, USA, 30–40.

Ihaka, R., Gentleman, R. and Team, R. D. C. (1997). *The R Project for Statistical Computing*. Internet. Retrievable at http://www.r-project.org.

J Wu, Y. J. T., H Z Deng and Zhu, D. Z. (2007). Vulnerability of complex networks under intentional attack with incomplete information. *Journal of Physics A: Mathematical and Theoretical*. 40, 2665–2671.

Jacobs, S. and Corson, S. (1999). *MANET authentication architecture*. Internet draft (draft-jacobs-imep-auth-arch-01.txt).

Jiejun Kong, M. G., Xiaoyan Hong (2003). *An Anonymous On Demand Routing Protocol with Untraceable Routes for Mobile Ad-hoc Networks*. Technical report. University of California, Los Angeles, CA 90095: UCLA COMPUTER SCIENCE DEPARTMENT TECHNICAL.

Joa-Ng, M. and Lu, I.-T. (1999). A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*. 17(8), 1415–1425. doi:10.1109/49.779923.

Johnson, D., Y.Hu and D.Maltz (2007). *The Dynamic Source Routing Protocol (DSR) for mobile Ad hoc network for IPV4*. Request for Comments 4728 (rfc4728.txt). Retrievable at http://www.ietf.org/rfc/rfc4728.txt.

Johnson, D. A., David B.and Maltz (1996). Dynamic Source Routing in Ad Hoc Wireless Networks. In Imielinski and Korth (Eds.) *Mobile Computing*. vol. 353. Kluwer Academic Publishers. Retrievable at http://citeseer.ist.psu.edu/johnson96dynamic.html.

Jou, Y. F., Gong, F., Sargor, C., Wu, X., Wu, S. F., Chang, H. C. and Wang, F. (2000). Design and Implementation of a Scalable Intrusion Detection System for the Protection of Network Infrastructure. In *Proceedings of the DARPA Information Survivability Conference and Exposition*. January. 25–27.

Junhai, L., Danxia, Y., Liu, X. and Mingyu, F. (2009). A survey of multicast routing protocols for mobile Ad-Hoc networks. *IEEE Communications Surveys & Tutorials*. 11(1), 78–91. doi:10.1109/SURV.2009.090107.

Kachirski, O. and Guha, R. (2003). Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03*, vol. 2. 6-9 Jan. 2003. IEEE Computer Society Washington, DC, USA, 57.1.

Kadri, B., Feham, M. and M'hamed, A. (2009). Securing reactive routing protocols in MANETs using PKI (PKI-DSR). *Security and Communication Networks Security Comm. Networks*. 2(4), 341–350.

Khabbazian, M., Mercier, H. and Bhargava, V. (2009). Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks. *Wireless Communications, IEEE Transactions on*. 8(2), 736 –745. ISSN 1536-1276. doi:10.1109/TWC.2009.070536.

Khalil, I., Bagchi, S. and Shroff, N. B. (2007). LiteWorp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Computer Networks*. 51(13), 3750 – 3772. ISSN 1389-1286. doi:DOI:10.1016/j.comnet.2007.04.001. Retrievable at http://www.sciencedirect.com/science/article/pii/S1389128607001004.

Ko, Y.-B. and Vaidya, N. H. (2000). Location-aided routing (LAR) in mobile ad hoc networks. *Wireless Networks*. 6(4), 307–321. ISSN 1022-0038. doi:http://dx.doi.org/10.1023/A:1019106118419.

Kohavi, R. and Provost, F. (1998). Glossary of Terms. *Machine Learning*. 30, 271–274. ISSN 0885-6125. Retrievable at http://dx.doi.org/10.1023/A:1017181826899.

Komninos, N. and Douligeris, C. (2009). LIDF: Layered intrusion detection framework for ad-hoc networks. *Ad Hoc Networks*. 7(1), 171 – 182. ISSN 1570-8705. doi:DOI:10.1016/j.adhoc.2008.01.001. Retrievable at http://www.sciencedirect.com/science/article/B7576-4RKMJ3K-1/2/876250a7b4032553b0b721739614d59c.

Komninos, N., Vergados, D. and Douligeris, C. (2006). Layered security design for mobile ad hoc networks. *Computers & Security*. 25(2), 121 – 130. ISSN 0167-4048. doi:DOI:10.1016/j.cose.2005.09.005. Retrievable at http://www.sciencedirect.com/science/article/B6V8G-4HHWVYN-2/2/b8d319505692b34980b6ba944540ca75.

Komninos, N., Vergados, D. D. and Douligeris, C. (2007). Authentication in a layered security approach for mobile ad hoc networks. *Computers & Security*. 26(5), 373 – 380. ISSN 0167-4048. doi:DOI:10.1016/j.cose.2006.12.011. Retrievable at http://www.sciencedirect.com/science/article/B6V8G-4MS3J7D-1/2/2fb0c222866ba1ff0b865ac051aeb807.

Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A. and Nemoto, Y. (2007). Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. *International Journal of Network Security*. Vol.5(No.3), 338–346.

Kwon, T. (2002). Impersonation attacks on software-only two-factor authentication schemes. *Communications Letters, IEEE*. 6(8), 358 – 360. ISSN 1089-7798. doi:10.1109/LCOMM.2002.802034.

Lamport, L. (1981). Password authentication with insecure communication. *Commun. ACM*. 24, 770–772. ISSN 0001-0782. doi:http://doi.acm.org/10.1145/358790.358797. Retrievable at http://doi.acm.org/10.1145/358790.358797.

Lauf, A. P., Peters, R. A. and Robinson, W. H. (2010). A distributed intrusion detection system for resource-constrained devices in ad-hoc networks. *Ad Hoc Networks*. 8(3), 253 – 266. ISSN 1570-8705. doi:DOI:10.1016/j.adhoc.2009.08.002. Retrievable at http://www.sciencedirect.com/science/article/B7576-4X1J75D-1/2/4171d1b159ebf5c243ea6adef75bb193.

Le Boudec, J.-Y. (2010). *Performance Evaluation of Computer and Communication Systems*. EPFL Press, Lausanne, Switzerland. Retrievable at http://perfeval.epfl.ch/.

Liang, W. and Wang, W. (2005). On performance analysis of challenge/response based authentication in wireless networks. *Computer*

Networks. 48(2), 267 – 288. ISSN 1389-1286. doi:DOI:10.1016/j.comnet.2004.10.016. Retrievable at http://www.sciencedirect.com/science/article/B6VRG-4F4R144-5/2/e431b56ed28e799aaf22d2a6d5f6aae2.

Lima, M., dos Santos, A. and Pujolle, G. (2009). A survey of survivability in mobile ad hoc networks. *Communications Surveys Tutorials, IEEE*. 11(1), 66 –77. ISSN 1553-877X. doi:10.1109/SURV.2009.090106.

Lu, S., Li, L., Lam, K.-Y. and Jia, L. (2009). SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack. In *Proc. Int. Conf. Computational Intelligence and Security CIS '09*, vol. 2. 421–425. doi:10.1109/CIS.2009.244.

Marti, S., Giuli, T. J., Lai, K. and Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*. MobiCom '00. New York, NY, USA: ACM. ISBN 1-58113-197-6, 255–265. doi:http://doi.acm.org/10.1145/345910.345955. Retrievable at http://doi.acm.org/10.1145/345910.345955.

Merkle, R. C. (1980). Protocols for Public Key Cryptosystems. In *IEEE Symposium on Security and Privacy*. April. 122–134.

Merkle, R. C. (1989). A certified digital signature. In *Proceedings on Advances in cryptology*. CRYPTO '89. New York, NY, USA: Springer-Verlag New York, Inc. ISBN 0-387-97317-6, 218–238. Retrievable at http://portal.acm.org/citation.cfm?id=118209.118230.

Michael A. Babyak, P. (2004). What you See May Not be What You Get: A brief, Nontechnical Introduction to Overfitting in Regression-Type Models. *Journal Of Biobehavioral Medice - Psychosomatic Medicine*. 66, 411–421.

Michiardi, P. and Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*. Deventer, The Netherlands, The Netherlands: Kluwer, B.V. ISBN 1-4020-7206-6, 107–121.

Mishra, A., Nadkarni, K. and Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. *Wireless Communications, IEEE*. 11(1), 48–60. ISSN 1536-1284. doi:10.1109/MWC.2004.1269717.

Mnaouer, A. B., Chen, L., Foh, C. H. and Tantra, J. W. (2007). OPHMR: An Optimized Polymorphic Hybrid Multicast Routing Protocol for MANET.

IEEE TRANSACTIONS ON MOBILE COMPUTING. 6(5), 551–562. doi: 10.1109/TMC.2007.1030.

Moineddin, R. (2001). *Comments on Mallows' Cp Statics And Multicollinearity Effects On Predcions*. Master's Thesis. University of Toronto Canada.

Murthy, S. and Garcia-Luna-Aceves, J. (1996). An efficient routing protocol for wireless networks. *Mobile Networks and Applications*. 1, 183–197. ISSN 1383-469X. Retrievable at http://dx.doi.org/10.1007/BF01193336.

Nait-Abdesselam, F. (2008). Detecting and avoiding wormhole attacks in wireless ad hoc networks. *IEEE Communications Magazine*. 46(4), 127–133. doi:10.1109/MCOM.2008.4481351.

Nguyen, H. L. and Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. *Ad Hoc Networks*. 6(1), 32 – 46. ISSN 1570-8705. doi:DOI:10.1016/j.adhoc.2006.07.005. Retrievable at http://www.sciencedirect.com/science/article/B7576-4KSJXYM-1/2/4fe7189021fa4955f6f893e3ee5d583d.

Nikaein, N., Bonnet, C. and Nikaein, N. (2001). Harp - Hybrid Ad-Hoc Routing Protocol. In *Proceedings of IST: International Symposium on Telecommunications*. September. Retrievable at http://citeseerx.ist.psu.edu/viewdoc/summary;jsessionid=BEB14F3FC85F8DC055C1F2B2053DD398?doi=10.1.1.9.5339.

Northcutt, S., Zeltser, L., Winters, S., Kent, K. and Ritchey, R. W. (2005). *Inside Network Perimeter Security*. Sams Publishing.

Pani, N. K. (2009). *A Secure Zone-Based Routing Protocol For Mobile Ad Hoc Networks*. Master's Thesis. National Institute of Technology, Rourkela - India.

Papadimitratos, P. and Haas, Z. J. (2002). Secure routing for mobile ad hoc networks. In *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS)*. January. San Antonio, TX, 27–31.

Park, B.-N. and Lee, W. (2005). ISMANET: A Secure Routing Protocol Using Identity-Based Signcryption Scheme for Mobile Ad-Hoc Networks. *IEICE Transactions*. 88-B(6), 2548–2556.

Park, B.-N., Myung, J. and Lee, W. (2005). LSRP: A Lightweight Secure Routing Protocol with Low Cost for Ad-Hoc Networks. In Kim, C. (Ed.) *Information Networking. Convergence in Broadband and Mobile Networking*. (pp. 160–169). *Lecture Notes in Computer Science*, vol. 3391. Springer Berlin / Heidelberg. Retrievable at http://dx.doi.org/10.1007/978-3-540-30582-8_17.

Park, V. and Corson, S. (2001). *Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification*. Functional Specification draft-ietf-manet-tora-spec-04 (draft-ietf-manet-tora-spec-04.txt). Retrievable at https://datatracker.ietf.org/doc/draft-ietf-manet-tora-spec/.

Pearlman, M. and Haas, Z. (1999). Determining the optimal configuration for the zone routing protocol. *Selected Areas in Communications, IEEE Journal on Selected Areas in Communications, IEEE Journal on*. 17(8), 1395–1414.

Pei, G., Gerla, M. and Chen, T.-W. (2000). Fisheye State Routing in Mobile Ad Hoc Networks. In *Proceedings of ICDCS Workshop on Wireless Networks and Mobile Computing, April 2000, Taipei, Taiwan*. April. ICDCS, D71–D78. Retrievable at http://www.cs.ucla.edu/NRL/wireless/PAPER/pei-wnmc00.ps.gz.

Pei, G., Gerla, M., Hong, X. and Chiang, C.-C. (1999). A wireless hierarchical routing protocol with group mobility. In *IEEE Wireless Communications and Networking Conference, WCNC1999, September 1999, New Orleans, LA, USA*. 1. September. IEEE, IEEE, 1538–1542. Retrievable at http://www.cs.ucla.edu/NRL/wireless/PAPER/wcnc99.pdf.gz.

Perkins, C. and Royer, E. (1999). Ad-hoc on-demand distance vector routing. In *Proceedings WMCSA '99. Second IEEE Workshop on Mobile Computing Systems and Applications*. Feb. 90–100. doi:10.1109/MCSA.1999.749281.

Perkins, C. E. and Bhagwat, P. (1994). Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. *SIGCOMM Comput. Commun. Rev.* 24(4), 234–244. ISSN 0146-4833. doi:http://doi.acm.org/10.1145/190809.190336.

Perkins, C. E., Royer, E. B. and S.Das (2003). *Ad hoc On-Demand Distance Vector (AODV) Routing*. Request for Comments 3561 (rfc3561.txt). Retrievable at http://www.ietf.org/rfc/rfc3561.txt.

Perrig, A., Canetti, R., Tygar, J. and Song, D. (2000). Efficient authentication and signing of multicast streams over lossy channels. In *Security and Privacy, 2000. S P 2000. Proceedings. 2000 IEEE Symposium on*. 56 –73. doi:10.1109/SECPRI.2000.848446.

Petter Holme, C. N. Y. S. K. H., Beom Jun Kim (2002). Attack Vulneratility of Complex Networkss. *Physical Review E*. 65, 1–15.

Poovendran, R. and Lazos, L. (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wirel. Netw.* 13(1), 27–59. ISSN 1022-0038. doi:http://dx.doi.org/10.1007/s11276-006-3723-x.

Qian, L., Song, N. and Li, X. (2007). Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach. *Journal of Network and Computer Applications*. 30(1), 308 – 330. ISSN 1084-8045. doi:DOI:10.1016/j.jnca.2005.07.003. Retrievable at http://www.sciencedirect.com/science/article/B6WKB-4H0RYYD-1/2/98e60cdf806d75534ed2387ad64d8a00.

Raffo, D., Adjih, C., Clausen, T. and M., P. (2004). An advanced signature system for OLSR. In *Proceedings of the 2nd ACM workshop on Security ad hoc and sensor networks: SASN '04*. New York, NY, USA: ACM. ISBN 1-58113-972-1, 10–16. doi:http://doi.acm.org/10.1145/1029102.1029106.

Ramachandran, P. and Yasinsac, A. (2004). Limitations of on demand secure routing protocols. In *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*. June. 52 – 59. doi:10.1109/IAW.2004.1437797.

Ramakrishnan, M., Priya, S. and Shanmugavel, S. (2010). Mathematical Modeling of Routing Protocol Selection for Optimal Performance of MANET. In *Computer and Network Technology (ICCNT), 2010 Second International Conference on*. 217 –221. doi:10.1109/ICCNT.2010.59.

Ramasubramanian, V., Haas, Z. J. and Sirer, E. G. (2003). SHARP: a hybrid adaptive routing protocol for mobile ad hoc networks. In *MobiHoc '03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM. ISBN 1-58113-684-6, 303–314. doi:http://doi.acm.org/10.1145/778415.778450.

Ramaswami, S. S. and Upadhyaya, S. (2006). Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing. In *Proc. IEEE Information Assurance Workshop*. June. 253–260. doi:10.1109/IAW.2006.1652103.

Razak, S., Furnell, S., Clarke, N. and Brooke, P. (2008). Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks. *Ad Hoc Networks*. 6(7), 1151 – 1167. ISSN 1570-8705. doi:DOI:10.1016/j.adhoc.2007.11.004. Retrievable at http://www.sciencedirect.com/science/article/B7576-4R6B2P2-1/2/e67fd04f1bd949cf0644cdb1b87292e7.

Rechberger, C. and Rijmen, V. (2008). New Results on NMAC/HMAC when Instantiated with Popular Hash Functions. *Journal of Universal Computer Science*. 14(3), 347–376.

Rencher, A. C. and Schaalje, G. B. (2008). *Linear Models In Statistics*. (2nd ed.). ISBN: 978-0-471-75498-5. John Wiley & Sons, Inc.

Rivest, R. and Shamir, A. (1997). *PayWord and MicroMint: Two simple micropayment schemes*, Springer Berlin / Heidelberg, vol. 1189. 69–87.

Roblot, X.-F. (2004). Polynomial factorization algorithms over number fields. *Journal of Symbolic Computation*. 38(5), 1429 – 1443. ISSN 0747-7171. doi:DOI:10.1016/j.jsc.2004.05.002. Retrievable at http://www.sciencedirect.com/science/article/B6WM7-4CY0G09-1/2/887bce511a12d7d65dbba51f35709833.

Rogaway, P. and Shrimpton, T. (2004). Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. In *Lecture Notes in Computer Science, 2004*. (pp. 371–388). vol. 3017/2004. Springer. doi:10.1007/978-3-540-25937-4_24.

Rohatgi, P. (1999). A compact and fast hybrid signature scheme for multicast packet authentication. In *Proceedings of the 6th ACM conference on Computer and communications security*. CCS '99. New York, NY, USA: ACM. ISBN 1-58113-148-8, 93–100. doi:http://doi.acm.org/10.1145/319709.319722. Retrievable at http://doi.acm.org/10.1145/319709.319722.

Rohde, S. (2008). *Protocols and Light-Weight Algorithms for Wireless Authentication Through Side Channels in IEEE 802.11 Communication*. Master's Thesis. Ruhr-UniversitÃd't Bochum.

Roy, D., Chaki, R. and Chaki, N. (2010). BHIDS: a new, cluster based algorithm for black hole IDS. *Security and Communication Networks*. 3(2-3), 278–288. ISSN 1939-0114. Retrievable at ISI:000277157600013.

Samad, F. (2011). *Securing Wireless Mesh Networks âĂŞ A Three Dimensional Perspective*. Ph.D. Thesis. RWTH Aachen University, Germany.

Sangi, A., Liu, J. and Zou, L. (2009). A Performance Analysis of AODV Routing Protocol under Combined Byzantine Attacks in MANETs. In *Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on*. December. 1 –5. doi:10.1109/CISE.2009.5366608.

Santos, O. (2007). *End-to-End Network Security: Defense-in-Depth*. Cisco Press.

Sanzgiri, K., Dahill, B., Levine, B., Shields, C. and Belding-Royer, E. (2002). A secure routing protocol for ad hoc networks. In *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*. nov. ISSN 1092-1648, 78 – 87. doi:10.1109/ICNP.2002.1181388.

Sanzgiri, K., LaFlamme, D., Dahill, B., Levine, B., Shields, C. and Belding-Royer, E. (2005). Authenticated routing for ad hoc networks. *Selected Areas*

in Communications, IEEE Journal on. 23(3), 598 – 610. ISSN 0733-8716. doi:10.1109/JSAC.2004.842547.

SchwingenschlÃűgl, C., Eichler, S. and MÃijller-Rathgeber, B. (2006). Performance of PKI-based security mechanisms in mobile ad hoc networks. *AEU - International Journal of Electronics and Communications.* 60(1), 20 – 24. ISSN 1434-8411. doi:DOI:10.1016/j.aeue.2005.10.004. Retrievable at http://www.sciencedirect.com/science/article/B7GWW-4HHGNXS-1/2/0a8c03a27ad883ed46ea122c39e6f805.

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* 26(5), 1484–1509. ISSN 0097-5397. doi:http://dx.doi.org/10.1137/S0097539795293172.

Sivakumar, R., Sinha, P. and Bharghavan, V. (1999). CEDAR: a core-extraction distributed ad hoc routing algorithm. *Selected Areas in Communications, IEEE Journal on.* 17(8), 1454 –1465. ISSN 0733-8716. doi:10.1109/49.779926.

Smith, B. R., Murthy, S. and Garcia-Luna-Aceves, J. (1997). Securing Distance-Vector Routing Protocols. In *Proceedings of the 1997 Symposium on Network and Distributed System Security.* Washington DC, USA: IEEE Computer Society, 85.

Sola, J. and Sevilla, J. (1997). Importance of input data normalization for the application of neural networks to complex industrial problems. *Nuclear Science, IEEE Transactions on.* 44(3), 1464 –1468. ISSN 0018-9499. doi:10.1109/23.589532.

Steinwandt, R. and VillÃąnyi, V. I. (2008). A one-time signature using run-length encoding. *Information Processing Letters.* 108(4), 179 – 185. ISSN 0020-0190. doi:DOI:10.1016/j.ipl.2008.05.004. Retrievable at http://www.sciencedirect.com/science/article/B6V0F-4SHVSYX-1/2/cb8143504f0d3ceeb8c7432e00ea94d3.

Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C., Balupari, R., Tseng, C.-Y., Bowen, T., Levitt, K. and Rowe, J. (2005). A General Cooperative Intrusion Detection Architecture for MANETs. In *Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA '05).* Washington, DC, USA: IEEE Computer Society. ISBN 0-7695-2317-X, 57–70. doi:http://dx.doi.org/10.1109/IWIA.2005.1.

Su, M.-Y. (2010). WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. *Computers & Security.* 29(2), 208 – 224. ISSN 0167-4048. doi:DOI:10.1016/j.cose.2009.09.

005. Retrievable at http://www.sciencedirect.com/science/article/B6V8G-4XFFJJK-2/2/616cf995987e730a3572aa8cd09acbde.

Su, M.-Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. *Computer Communications*. 34(1), 107 – 117. ISSN 0140-3664. doi:DOI:10.1016/j.comcom.2010.08.007. Retrievable at http://www.sciencedirect.com/science/article/B6TYP-50VTWM5-2/2/9b9b9e7b4e7627e9f8272c3895ca73f3.

Sun, B., Guan, Y., Chen, J. and Pooch, U. (2003a). Detecting black-hole attack in mobile ad hoc networks. In *Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492)*. April. ISSN 0537-9989, 490 – 495. doi:10.1049/cp:20030303.

Sun, B., Wu, K. and Pooch, U. W. (2003b). Alert aggregation in mobile ad hoc networks. In *Proceedings of the 2nd ACM workshop on Wireless security (WiSe '03)*. New York, NY, USA: ACM. ISBN 1-58113-769-9, 69–78. doi:http://doi.acm.org/10.1145/941311.941323.

Sun, D.-Z., Cao, Z.-F. and Sun, Y. (2005). Remarks on a new key authentication scheme based on discrete logarithms. *Applied Mathematics and Computation*. 167(1), 572 – 575. ISSN 0096-3003. doi:DOI:10.1016/j.amc.2004.07.021. Retrievable at http://www.sciencedirect.com/science/article/B6TY8-4DHXMY3-5/2/4e35f184abfd8d29d796692094810190.

Systems, T. C. and Technology Group, M. (2009). *DARPA data set*. Retrievable at http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html.

Tai, S., Luo, P., Peng, X. and Wang, D. (2005). Weak-Keys in Public Key Cryptosystems Based on Discrete Logarithms. *Tsinghua Science & Technology*. 10(5), 579 – 581. ISSN 1007-0214. doi:DOI:10.1016/S1007-0214(05)70121-8. Retrievable at http://www.sciencedirect.com/science/article/B7RKT-4H62D8B-B/2/b435c27c64405ca7f12c07aaa5d02e17.

Tamilselvan, L. and Sankaranarayanan, V. (2008). Prevention of Co-operative Black Hole Attack in MANET. *Journal of Networks*. 3, 13–20.

Teske, E. (2003). Computing discrete logarithms with the parallelized kangaroo method. *Discrete Applied Mathematics*. 130(1), 61 – 82. ISSN 0166-218X. doi:DOI:10.1016/S0166-218X(02)00590-5. Retrievable at http://www.sciencedirect.com/science/article/B6TYW-490RGGK-3/2/340fa8ea4ccd214541cf9534ca795a31, the 2000 Com2MaC Workshop on Cryptography.

The Bouncy Castle, T. L. o. (2010). *Bouncy Castle Provider*. Retrievable at http://www.bouncycastle.org, site hosted by Tau Ceti Co-operative Ltd.

Thomas Clausen, U. H. (2010). *Vulnerability Analysis of the Optimized Link State Routing Protocol version 2 (OLSRv2)*. Technical report. INRIA.

Toh, C.-K. (1996). A novel distributed routing protocol to support ad-hoc mobile computing. mar. 480 –486. doi:10.1109/PCCC.1996.493675.

Tonnesen, A. (2004). *Impementing and extending the Optimized Link State Routing Protocol*. Technical report. UniK University Graduate Center University of Oslo. Retrievable at www.olsr.org/docs/report.pdf.

Tran, P. V., Hung, L. X., Lee, Y.-K., Lee, S. and Lee, H. (2007). TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks. In *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*. 593 –598. doi:10.1109/CCNC.2007.122.

Tseng, C.-Y. H. (2006). *Distributed Intrusion Detection Models for Mobile Ad Hoc Networks*. Ph.D. Thesis. UNIVERSITY OF CALIFORNIA - DAVIS.

Tseng, C.-Y. H., Balasubramanyam, P., Ko, C., Limprasittiporn, R., Rowe, J. and Levitt, K. (2003). A specification-based intrusion detection system for AODV. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, SASN '03*. New York, NY, USA: ACM. ISBN 1-58113-783-4, 125–134. doi:http://doi.acm.org/10.1145/986858.986876.

University of California, I. (2009). *KDD 99 Task*. Retrievable at http://kdd.ics.uci.edu/databases/kddcup99/task.html.

Vahdat, A. and Becker, D. (2000). *Epidemic Routing for Partially-Connected Ad Hoc Networks*. Technical Report CS-2000-06. Duke University. Retrievable at http://issg.cs.duke.edu/epidemic/epidemic.pdf.

Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, E. M. and Kemmerer, R. A. (2004). An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks. In *ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference*. Washington, DC, USA: IEEE Computer Society. ISBN 0-7695-2252-1, 16–27. doi:http://dx.doi.org/10.1109/CSAC.2004.6.

Vu, H., Kulkarni, A., Sarac, K. and Mittal, N. (2008). WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks. In *WASA '08: Proceedings of the Third International Conference on Wireless Algorithms, Systems, and Applications*. October. Berlin, Heidelberg: Springer-Verlag. ISBN 978-3-540-88581-8, 491–502. doi:http://dx.doi.org/10.1007/978-3-540-88582-5_46.

Wallace, D. and White, W. (2008). Pseudoprime factorizations of integer matrices. *Linear Algebra and its Applications*. 429(1), 142 – 155. ISSN 0024-3795. doi:DOI:10.1016/j.laa.2008.02.012. Retrievable at http://www.sciencedirect.com/science/article/B6V0R-4S80D16-1/2/2ef14917fc44421003b5c8aef61cf647.

Wang, L. and Olariu, S. (2004). A two-zone hybrid routing protocol for mobile ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems*. 15(12), 1105–1116. doi:10.1109/TPDS.2004.73.

Wang, P., Reeves, D. and Ning, P. (2005). Secure address auto-configuration for mobile ad hoc networks. In *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*. jul. 519 – 521. doi:10.1109/MOBIQUITOUS.2005.52.

Weerasinghe, H. and Fu, H. (2008). Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation. *International Journal of Software Engineering and Its Applications*. Vol. 2(No. 3), 39–54.

Weisberg, S. (2005). *Applied Linear Regression*. (3rd ed.). ISBN:0-471-66379-4. John Wiley & Sons.

Wu, B., Chen, J., Wu, J. and Cardei, M. (2007). A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In Xiao, Y., Shen, X. S. and Du, D.-Z. (Eds.) *Wireless Network Security*. (pp. 103–135). Signals and Communication Technology. Springer US. ISBN 978-0-387-33112-6. Retrievable at http://dx.doi.org/10.1007/978-0-387-33112-6_5.

Xiang, X., Wang, X. and Yang, Y. (2010). Stateless Multicasting in Mobile Ad Hoc Networks. *IEEE Transactions on Computers*. 59(8), 1076–1090. doi:10.1109/TC.2010.102.

Yang, H., Luo, H., Ye, F., Lu, S. and Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. *Wireless Communications, IEEE*. 11(1), 38 – 47. ISSN 1536-1284. doi:10.1109/MWC.2004.1269716.

Yi, P., Dai, Z., Zhang, S. and Zhong, Y. (2005). A New Routing Attack in Mobile Ad Hoc Networks. *International Journal of Information Technology*. 11, 83–94.

Yi, S., Naldurg, P. and Kravets, R. (2001). Security-aware ad hoc routing for wireless networks. In *MobiHoc '01: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*. New York, NY, USA: ACM. ISBN 1-58113-428-2, 299–302.

Yi, S., Yi, S. and Kravets, R. (2003). MOCA : Mobile Certificate Authority for Wireless Ad Hoc Networks. In *2nd Annual PKI Research Workshop Program (PKI 03)*. April 28-29. 65–79.

Yoo, Y. and Agrawal, D. P. (2006). Why does it pay to be selfish in a MANET? *Wireless Communications, IEEE*. 13(6), 87 –97. ISSN 1536-1284. doi:10.1109/MWC.2006.275203.

Zapata, M. G. (2006a). Key management and delayed verification for ad hoc networks. *J. High Speed Netw.* 15, 93–109. ISSN 0926-6801. Retrievable at http://portal.acm.org/citation.cfm?id=1140563.1140570.

Zapata, M. G. (2006b). *Secure Ad hoc On-Demand Distance Vector (SAODV) Routing*. INTERNET-DRAFT (draft-guerrero-manet-saodv-06.txt). Retrievable at http://ietfdocs.potaroo.net/all-ids/draft-guerrero-manet-saodv-06.txt.

Zapata, M. G. and Asokan, N. (2002). Securing ad hoc routing protocols. In *Proceedings of the 1st ACM workshop on Wireless security*. December. New York, NY, USA: ACM, 1–10.

Zhai, W. (2009). On the prime power factorization of n! *Journal of Number Theory*. 129(8), 1820 – 1836. ISSN 0022-314X. doi:DOI:10.1016/j.jnt.2009.02.016. Retrievable at http://www.sciencedirect.com/science/article/B6WKD-4W7B57M-2/2/ddef26a9b993bf4989137b6a129c2b38.

Zhang, J. and Zulkernine, M. (2006). A hybrid network intrusion detection technique using random forests. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*. april. 8 pp. doi:10.1109/ARES.2006.7.

Zhang, K. (1998). Efficient Protocols for Signing Routing Messages. In *Proceedings of 1998 Internet Society Symposium on Network and Distributed System Security (NDSS'98)*.

Zhang, X., Neglia, G., Kurose, J. and Towsley, D. (2007). Performance modeling of epidemic routing. *Computer Networks*. 51(10), 2867 – 2891. ISSN 1389-1286. doi:DOI:10.1016/j.comnet.2006.11.028. Retrievable at http://www.sciencedirect.com/science/article/B6VRG-4MM1P6H-4/2/d53aa3214d4ce3ac3f29fe22096e4742.

Zhang, Y. and Lee, W. (2005). Security in Mobile Ad-Hoc Networks. In Mohapatra, P. and Krishnamurthy, S. V. (Eds.) *Ad Hoc Networks*. (pp. 249–268). Springer US. ISBN 978-0-387-22690-3.

Zhang, Y., Lee, W. and Huang, Y.-A. (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Networks*. 9(5), 545–556. ISSN 1022-0038. doi:http://dx.doi.org/10.1023/A:1024600519144.

Zhen, J. and Srinivas, S. (2003). Preventing Replay Attacks for Secure Routing in Ad Hoc Networks. In Pierre, S., Barbeau, M. and Kranakis, E. (Eds.) *Ad-Hoc, Mobile, and Wireless Networks*. (pp. 140–150). *Lecture Notes in Computer Science*, vol. 2865. Springer Berlin / Heidelberg.

Zhou, J. and Lam, K. Y. (1999). Securing digital signatures for non-repudiation. *Computer Communications*. 22(8), 710 – 716. ISSN 0140-3664. doi:DOI: 10.1016/S0140-3664(99)00031-6.

Zhou, L. and Haas, Z. (1999). *Securing Ad Hoc Networks*. Technical Report TR99-1772. Ithaca, NY, USA: Cornell University.

Zouridaki, C., Mark, B. L., Gaj, K. and Thomas, R. K. (2004). Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography. In Katsikas, S. K., Gritzalis, S. and Lopez, J. (Eds.) *Public Key Infrastructure*. (pp. 623–623). *Lecture Notes in Computer Science*, vol. 3093. Springer Berlin / Heidelberg.