UNIVERSITI PUTRA MALAYSIA

WORMHOLE ATTACK DETECTION MECHANISM IN MOBILE AD HOC NETWORK USING NEIGHBORHOOD INFORMATION AND PATH TRACING ALGORITHM

MEHDI ENSHAEI

FSKTM 2015 7

WORMHOLE ATTACK DETECTION MECHANISM IN MOBILE AD HOC NETWORK USING NEIGHBORHOOD INFORMATION AND PATH TRACING ALGORITHM

By

MEHDI ENSHAEI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Master of Science

October 2015

DEDICATIONS

I THANK MY GOD WHOSE BLESSINGS HAVE MADE IT ALL POSSIBLE IN THE FIRST PLACE.

This thesis is dedicated to:

My Father

My Mother

My Sister

And my Lovely Wife

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

WORMHOLE ATTACK DETECTION MECHANISM IN MOBILE AD HOC NETWORK USING NEIGHBORHOOD INFORMATION AND PATH TRACING ALGORITHM

By

MEHDI ENSHAEI

October 2015

Chair: Zurina Mohd Hanapi, PhD
Faculty: Computer Science and Information Technology

Mobile Ad hoc Networks (MANETs) is a self-configuring network that is formed automatically by a collection of mobile nodes. Security is often the major concern as MANET does not rely on a centralized administration. A mobile node cannot have single hop communication with the destination, due to low transmission range of the nodes. Therefore, MANET depends on intermediate nodes to forward messages to the destination, and willing to forward a message to other nodes without being selfish. MANET is vulnerable to attacks due to the open, cooperative and dynamic nature and needs a new method for secure communication. Wormhole attack is one of the dangerous attacks in MANET in which two or more destructive nodes record the packets at one point, to another point in the network. Wormhole attack detection is very hard, even; the use of cryptographic technique is not enough to prevent it as the wormhole attackers do not create separate packets, but simply replay packets that already exist on the network by passing all cryptographic checks. Path Tracing (PT) Algorithm was proposed to detect and prevent exposed wormhole attacks in MANET. This algorithm is good for MANET as they not have centralized management and autonomous mobile nodes connect with each other through the air. However, lack of distance calculation seems to be a major drawback of the PT algorithm. Impact of lack in distance calculation is nodes cannot decide whether the faraway node is malicious node or normal node. In this study, a new defence mechanism is proposed based on modification of the packet forwarding process, using Neighborhood Information (NI) and PT algorithm, and known as NIPT algorithm. Neighborhood Information is one

of the detection methods and it is under the category of neighbor discovery. Moreover, by checking acknowledge (ACK) packet by source node and confirm whether it belongs to the 1-hop neighbor or 2-hop neighbor, it is able to detect the wormhole in early stage. The study investigates in four different scenarios and detects both types of wormhole attacks. Experimental evaluation shows that NIPT algorithm achieves better results in the PDR and delay with an average of 5% and 6% respectively, over the PT algorithm. Throughput and packet overhead is improved in the NIPT algorithm with an average of 4% and 6% respctively over the PT algorithm. Wormhole attack caused a packet drops and indirectly impact the PDR, packet overhead, and packet delay. NIPT algorithm has better improvement on delay which presents the elimination of attacker. Using the NIPT, the packet drop is decreased and chosen the best route is free from the wormhole. At the same time, throughput decreases as the amount of malevolent nodes increase, however NIPT can detect wormhole attack earlier compare to PT. NIPT works better than PT, which helps the nodes know the distance and location of each other, where can detect wormhole easier and earlier, and no need to use hardware implementation.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master of Sains

MEKANISME PENGESAN SERANGAN LUBANG ULAT DALAM RANGKAIAN MUDAH ALIH AD HOC DENGAN MENGGUNAKAN ALGORITMA MAKLUMAT KEJIRANAN DAN PENJEJAKAN LALUAN

Oleh

MEHDI ENSHAEI

Oktober 2015

Pengerusi: Zurina Mohd Hanapi, PhD
Fakulti: Sains Komputer dan Teknolologi Maklumat

Rangkaian Mudah Alih Ad Hoc (MANETs) ialah rangkaian konfigurasi sendiri yang terbentuk secara automatik oleh koleksi nod mudah alih. Keselamatan sering menjadi keutamaan memandangkan MANET tidak bergantung pada pentadbiran berpusat. Nod mudah alih tidak boleh mempunyai komunikasi hop tunggal dengan destinasi, kerana julat penghantaran nod adalah rendah. Oleh itu, MANET bergantung kepada nod perantaraan untuk menghantar mesej ke destinasi, dan bersedia untuk menghantar mesej kepada nod lain tanpa mementingkan diri sendiri. MANET terdedah kepada serangan kerana sifat terbuka, saling membantu, dan dinamik yang memerlukan satu kaedah baru bagi komunikasi yang selamat. Serangan lubang ulat adalah salah satu serangan berbahaya di MANET yang mana dua atau nod yang lebih bahaya merekod paket pada satu titik ke titik yang lain dalam rangkaian. Pengesanan serangan lubang ulat adalah sangat sukar, walaupun dengan penggunaan teknik kriptografi yang mana masih tidak cukup untuk mencegahnya memandangkan penyerang lubang cacing tidak mencipta paket berasingan, tetapi hanya memainkan semula paket yang sudah wujud di rangkaian dengan melepasi semua semakan kriptografi. Algoritma Laluan mengesan (PT) yang telah dicadangkan bagi mengesan dan mencegah serangan lubang cacing yang terdedah di MANET. Algoritma ini bagus untuk MANET kerana ia tidak mempunyai pengurusan berpusat dan nod bimbit autonomi menyambung antara satu sama lain melalui udara. Walau bagaimanapun, kekurangan pengiraan jarak seolah-olah menjadi kelemahan utama algoritma PT. Kesan daripada kurang pengiraan jarak, nod tidak boleh membuat keputusan sama

ada nod jauh adalah nod berniat jahat atau nod normal. Dalam kajian ini, satu mekanisme pertahanan baru dicadangkan berdasarkan pengubahsuaian proses penghantaran paket, menggunakan Maklumat Kejiranan (NI) dan algoritma PT, dan dikenali sebagai algoritma NIPT. Maklumat kejiranan adalah salah satu kaedah pengesanan dan ia adalah di bawah kategori penemuan jiran. Di samping itu, dengan memeriksa paket akuan(ACK) oleh nod sumber dan mengesahkan sama ada ia milik jiran 1-hop atau 2-hop jiran, ia mampu untuk mengesan lubang ulat pada peringkat awal lagi. Kajian ini menyiasat empat senario yang berbeza dan mengesan kedua-dua jenis serangan lubang ulat. Penilaian eksperimen menunjukkan bahawa algoritma NIPT mencapai keputusan yang lebih baik dalam PDR dan kelewatan dengan purata 5% dan 6% masing-masing, berbanding algoritma PT. Pemprosesan dan paket overhed bertambah baik dalam algoritma NIPT dengan purata 4% dan 6% masing-masing berbanding algoritma PT. Serangan lubang ulat menyebabkan paket menurun dan secara tidak langsung memberi kesan kepada PDR, overhead paket, dan kelewatan paket. Algoritma NIPT mempunyai peningkatan lebih baik dalam kelewatan yang menunjukkan penghapusan penyerang. Menggunakan NIPT, penurunan paket berkurangan dan pilihan laluan yang terbaik adalah bebas daripada lubang ulat. Pada masa yang sama, pemprosesan berkurangan apabila jumlah nod jahat meningkat, walau bagaimanapun NIPT dapat mengesan serangan lubang ulat lebih awal berbanding dengan PT. NIPT berfungsi lebih baik daripada PT, yang membantu nod untuk mengetahui jarak dan lokasi antara satu sama lain, di mana boleh mengesan lubang ulat dengan mudah dan lebih awal, dan tanpa menggunakan implementasi perkakasan.

ACKNOWLEDGEMENTS

In the name of GOD, is the most gracious and merciful. I thank GOD for giving me the patient and strength to complete this research work I would like to acknowledge the efforts of my major advisor, Dr. Zurina Mohd Hanapi, in motivating and guiding me during my graduate study. I have been learning from her the principles as an investigator.

I would like to thank Professor Dr. Mohamed Othman his valuable advices. His precious time and feed-backs are greatly appreciated. His expertise and insight are the keys for the success of his students. I would like to acknowledge the assistance of some former/current graduate students in the FSKTM lab and specially Mohammed Ahmed Al Maqri and Ameen Mohammed Alkharasani.

I greatly appreciate the support and encouragement from my loving wife Maral Faghani Hamadani, she helped me to overcome the many difficulties on the way to completing this research work. I will never forget her supports.

Last but not least, my heartfelt thanks to my parents for their love, prayers, support and motivation which guided me through this long journey towards earning my Master.

I certify that a Thesis Examination Committee has met on 23 October 2015 to conduct the final examination of Mehdi Enshaei on his thesis entitled "Wormhole Attack Detection Mechanism in Mobile Ad Hoc Network Using Neighborhood Information and Path Tracing Algorithm" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Rohaya binti Latip, PhD
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Zuriati binti Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Abdul Hanan Abdullah, PhD
Professor
Universiti Teknologi Malaysia
Malaysia
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 15 December 2015

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Sciense.

The members of the Supervisory Committee were as follows:

Zurina Mohd Hanapi, Ph.D
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairperson)

Mohamed Othman, Ph.D
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

BUJANG KIM HUAT, Ph.D.
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: ———————— Date:————————-

Name and Matric No.: Mehdi Enshaei (GS34876)

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (graduate studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____
Name of
Chairman of
Supervisory
Committee: Zurina Mohd Hanapi, Ph.D

Signature: _____
Name of
Member of
Supervisory
Committee: Mohamed Othman, Ph.D

TABLE OF CONTENTS

		Page
ABSTRACT		i
ABSTRAK		iii
ACKNOWLEDGEMENTS		v
APPROVAL		vi
DECLARATION		viii
LIST OF TABLES		xii
LIST OF FIGURES		xiii
LIST OF ABBREVIATIONS		xiv
CHAPTER		
1	**INTRODUCTION**	1
	1.1 Background	1
	1.2 Problem Statement	1
	1.3 Research Objective	2
	1.4 Research Scope	2
	1.5 Contribution of Thesis	2
	1.6 Thesis Organization	3
2	**LITERATURE REVIEW**	4
	2.1 Mobile Ad hoc Network	4
	2.1.1 Features of MANETs	4
	2.1.2 Security Issues of MANETs	5
	2.2 Classification of Attacks	6
	2.3 Classification of Wormholes	6
	2.3.1 Wormhole Attack	7
	2.3.2 Threats Due to Wormhole Attack	10
	2.3.3 Effects of Wormhole Attack	11
	2.4 Techniques Classification	12
	2.4.1 Round Trip Time Based	12
	2.4.2 Neighbor Discovery/Verification Based	12
	2.4.3 Hardware Based	13
	2.4.4 Clock Based	14
	2.4.5 Packet Leashes Based	14
	2.4.6 Time To Live Based	14
	2.5 Related Works	14
	2.6 Summary	20

3 **METHODOLOGY** 22
3.1 Introduction 22
3.2 Research Framework 22
3.3 Experimental Environment 24
3.3.1 Hardware 24
3.3.2 Software 24
3.4 Existing Work: Path Tracing Algorithm 24
3.5 Neighborhood Information 25
3.6 Neighborhood Information and Path Tracing Algorithm 26
3.7 Performance Metrics 29
3.7.1 Wormhole Detection Rate 29
3.7.2 Packet Delivery Ratio 29
3.7.3 Throughput 29
3.7.4 Packet Overhead 30
3.7.5 Average Delay 30
3.7.6 Notations 30
3.7.7 Design 31
3.7.8 Flowchart Design 32
3.7.9 Broadcast HELLO Packet 34
3.7.10 ACK Response 36
3.7.11 Simulation Parameters 37
3.7.12 Assumptions 37
3.7.13 Network Model 38
3.8 Summary 41

4 **RESULTS AND DISCUSSION** 42
4.1 Introduction 42
4.2 NIPT Algorithm Results 42
4.2.1 Detection Rate of Wormhole Attack 42
4.2.2 Exposed Wormhole Attack 45
4.2.3 Hidden Wormhole Attack 48
4.2.4 Both Wormhole Attacks 51
4.2.5 Absence of Wormhole Attack 54
4.3 Summary 57

5 **CONCLUSION AND FUTURE WORK** 58
5.1 Conclusion 58
5.2 Future Work 59

REFERENCES 60
APPENDICES 67
BIODATA OF STUDENT 78
LIST OF PUBLICATIONS 79

LIST OF TABLES

Table		Page
2.1	MANET Attack Based on Network layers	6
2.2	Summary of Wormhole Detection Methods	18
3.1	Result of Neighbor Correctness Test	27
3.2	Notations Used in Equations	31
3.3	Simulation Parameters	38
C.1	Comparison Between the Wormhole Attacks	74

LIST OF FIGURES

Figure		Page
2.1	Typical MANET	4
2.2	Hidden and Exposed Wormhole	7
2.3	Demonstration of Wormhole Attack	8
2.4	Open Wormhole Attack	9
2.5	Closed Wormhole Attack	10
2.6	Node A's Immediate Neighborhood	12
3.1	Research Framework	23
3.2	Combination of NI and PT Algorithm	28
3.3	Flowchart NIPT	34
3.4	State Diagram NIPT Algorithm	36
3.5	Node S Sending Traffic to D Along P_{SD}	39
3.6	Drop Periodic Updates	40
3.7	Design of Network	40
3.8	Wormhole Nodes in Dense Network	41
3.9	Packet Drops in Network	42
4.1	Detection Rate of Wormhole Attack Based on Neighbors	44
4.2	Wormhole Detection Rate in NIPT	45
4.3	Wormhole Detection Rate in PT	45
4.4	Packet Delivery Ratio in Exposed Wormhole Attack	46
4.5	Throughput in Exposed Wormhole Attack	47
4.6	Packet Overhead in Exposed Wormhole Attack	48
4.7	Average Delay in Exposed Wormhole Attack	49
4.8	Packet Delivery Ratio in Hidden Wormhole Attack	50
4.9	Throughput in Hidden Wormhole Attack	51
4.10	Packet Overhead in Hidden Wormhole Attack	51
4.11	Average Delay in Hidden Wormhole Attack	52
4.12	Packet Delivery Ratio in Both Types of Wormhole Attacks	53
4.13	Throughput in Both Types of Wormhole Attacks	53
4.14	Packet Overhead in Both Types of Wormhole Attacks	54
4.15	Average Delay in Both types of Wormhole Attacks	55
4.16	Packet Delivery Ratio in Absence of Wormhole Attack	55
4.17	Throughput in Absence of Wormhole Attacks	56
4.18	Packet Overhead in Absence of Wormhole Attacks	56
4.19	Average Delay in Absence of Wormhole Attacks	57
A.1	Flowchart PT	68
A.2	State Diagram	69

LIST OF ABBREVIATIONS

ACK	Acknowledgement Packet
CA	Central Authority
CBR	Constant Bit Rate
CPU	Central Processing Unite
CTS	Clear to Send
DoS	Denial of Service
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
GPS	Global Positioning System
GPSR	Greedy Perimeter Stateless Routing
HMIT	HELLO Message Timing Intervals
LP3	Limiting Packet Propagation Parameter
MAC layer	Media Access Control layer
MAD	Mutual Authenticated Distance Bounding
MANET	Mobile Ad hoc Network
NAM	Network Animator
NAWA2	Neighbor Aware Wormhole Adversary Axing
NIPT	Neighborhood Information and Path Tracing
OLSR	Optimized Link State Routing protocol
OTCL	Object oriented Tool Command Language
PT	Path Tracing
RTS	Request to Send
QoS	Quality of Service
RREQ	Route Request Message
RREP	Route Reply Message
RTT	Round Trip Time
RWP	Random Way Point
SAM	Statistical Analysis of Multi-path
SHARP	Sharp Hybrid Adaptive Routing Protocol
SOLR	Secure Optimistic Link State Routing Protocol
TCP	Transmission Control Protocol
TCL	Tool Command Language
TIK	TESLA with Instant Key
TTL	Time To Live
WAP	Wormhole Attack Prevention
WARP	Wormhole Avoidance Routing Protocol
Wi-Fi	Wireless Fidelity
WRP	Wireless Routing
ZRP	Zone Routing Protocol

CHAPTER 1

INTRODUCTION

1.1 Background

In recent times, the rapid production of light and small portable gadgets such as PDAs, smart phones, and laptops, has lead to a latest category of mobile network named the Mobile Ad hoc Network (MANET). MANET is set of small range mobile nodes which communicate with other devices by air as medium, and this communication is done without having any infrastructure for routing packets (Lego and Sutradhar, 2011). Due to no existence of an infrastructure, nodes have responsibility to act as router or host to route the packets between each other. Ad hoc networks are employed in several useful scenarios such as battle fields, natural disasters to have temporary or emergency communication between mobile devices.

MANETs are principally important for conditions where deployment of infrastructure is precious or unreasonable, for example military operations, emergency rescue actions, live conference and university activity. Thus, security for these networks, is the main concern (Krishna et al., 2015). The open nature of MANETs or in the other hand, wireless transmission gives chance to outsiders to listen and control the network traffic or make interruption in network. Lack of centralized control authority makes difficulties for deployment security mechanism. It is very complex to implement perimeter-based defence system like firewalls due to the MANETs does not have clear point of entrance. Name of wormhole attack gets from physics, it consist of a narrow tube oface time which attaches far away areas of the cosmos. In network, wormhole attack behaves the same; two collaborating attackers create a tunnel and connect far parts of networks.

One side of attacker gets the traffic of one end of the network, and transmits the traffic by offline-channel link, to the other side of attacker. The second attacker re-broadcasts the traffic at the other network end. For ad hoc networks, wormhole attacks are in the group of dangerous attacks and it is very hard to be detected and prevented (Mishra and Singh, 2014) because cryptography-based measures do not improve them, as wormholes do not present new network messages, nor do the changes of available network messages.

1.2 Problem Statement

One of the important issues in wireless security is mobile nodes that have been extended in an un-trusted environment. The goal of the security mechanism is to detect the existence of wormholes that may be attracting the traffic. There are works done on security issues to detect the attacks such as wormhole attack in MANET, such as; (Anita et al., 2010) (Stoleru et al., 2012) (Patil et al., 2014). The Path Tracing (PT) algorithm introduced by Sakthivel and Chandrasekaran (2012), is one of the latest defence mechanism to detect

exposed wormhole attack in MANET. Where no additional requirements of hardware needed, that makes it more suitable for resource constrained. PT algorithm is using RTT, prior perhop distance, perhop distance and the number of participation of a link in a path to detect the exposed wormhole attack with greater throughput and less average delay and reduced overhead. The limitation of Path Tracing in the recent study by Anitha and Sivaganesh (2012) is the authors use criptography techniqe to detect wormhole attack however it is not proper for detection of hidden wormhole attack. Hidden wormhole attack did not change the header of the packet so they just detect exposed wormhole attack. Wormhole attack is very destructive since the neighborhood information is confused (Liu et al., 2014). Nodes use Neighborhood Information to detect the real neighbors. In the study by Lathies Bhasker (2013) authors used Neighborhood Information and just consider 1-hop and 2-hop neighbors and not check more than 2-hop. Even throughput, average delay and overhead can be used to measure impact of wormhole attack mechanism by identifying less throughput with high average delay and overhead. It means there is wormhole attack in the network, however it is still not enough because lacking of detection rate is obvious when calculate the wormhole detection rate in Path Tracing algorithm.

1.3 Research Objective

The objectives of this study are the followings:

- To design and develop effective defence mechanism to detect wormhole attacks using Neighborhood Information and Path Tracing algorithm.
- To achieave better detection rate, as well as achieve greater throughput and less average delay. In addition reduce packet overhead and improve packet delivery ratio.

1.4 Research Scope

This study is related to detection of wormhole attack by implementing only on Dynamic Source Routing protocol (DSR) In this implementation, the nodes make use of MAC protocol to gain access in radio transmission is not considered. At the same time, two different nodes do not have the same set of neighbors. The focus of this thesis only on whether the wormhole can be detected using the proposed defence mechanism.

1.5 Contribution of Thesis

This thesis deals with detection of wormhole attack in MANETs. This algorithm presents a novel mechanism to detect wormhole attack; rather than trying to detect packets travelled farther than they should or faster than they should (as other wormhole attack detection techniques do). The contribution of this study can be defined in details as follows:

In order to have the good defence mechanism, the Neighborhood Information (NI) and Path Tracing (PT) algorithm was proposed to have better detection rate and have better security in network. The defence mechanism is a combination of two approaches as mentioned; the mechanism use Round Trip Time (RTT) to get better results in terms of wormhole detection rate, and performance metrics such as; throughput, average delay, packet delivery ratio, and packet overhead in sparse and dense network. In order to avoid wormhole attack, the nodes participating in MANET communication have to be registered in the network. Each node has a unique ID which would help in maintaining the record of each participated node in the network.

1.6 Thesis Organization

The thesis includes five chapters. Chapter 1 presents a brief discussion on the background, problem statement, objectives, scopes, and findings of the research work.

Chapter 2 presents a literature study to review the main principles in MANETs, routing protocols, and related attacks such as wormhole attack which is the main focus of the thesis.

Chapter 3 explains the general research methodology used to accomplish the objective. It presents the framework of the research work and explores each stage in details. It covers the aspects of design of the mechanism, implementation, simulation parameters, and performance metrics.

Chapter 4 presents the simulation analysis and the results of the defence mechanism in four scenarios and in sparse and dense network.

Finally, this study is concluded and directions for future work are presented in Chapter 5.

REFERENCES

Ahuja, R., Ahuja, A. B. and Ahuja, P. 2013. Performance evaluation and comparison of AODV and DSR routing protocols in MANETs under wormhole attack. In Image Information Processing (ICIIP), 2013 IEEE Second International Conference on, 699–702. IEEE, Shimla, India.

Anita, E. M., Vasudevan, V. and Ashwini, A. 2010. A certificate-based scheme to defend against worm hole attacks in multicast routing protocols for MANETs. In Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on, 407–412. Ramanathapuram.

Anitha, P. and Sivaganesh, M. 2012. Detection and Prevention of Wormhole Attack in MANETS using Path Tracing. International Journal of communications and networking systems1 (2).

Azer, M. A., El-Kassas, S. M. and El-Soudani, M. S. 2009. Immuning routing protocols from the wormhole attack in wireless ad hoc networks. In Systems and Networks Communications, 2009. ICSNC'09. Fourth International Conference on, 30–36. IEEE.

Banerjee, S. and Majumder, K. 2014. WORMHOLE ATTACK MITIGATION IN MANET: A CLUSTER BASED AVOIDANCE TECHNIQUE. International Journal of Computer Networks & Communications 6 (1).

Bindra, H. S., Maakar, S. K. and Sangal, A. 2010. Performance evaluation of two reactive routing protocols of MANET using group mobility model. International Journal of Computer Science 7 (3): 38–43.

Buch, D. H. and Jinwala, D. 2011. Prevention of wormhole attack in wireless sensor network. arXiv preprint arXiv:1110.1928 .

Chen, H., Lou, W., Sun, X. and Wang, Z. 2010. A secure localization approach against wormhole attacks using distance consistency. EURASIP Journal on Wireless Communications and Networking2010: 8.

Chen, Q., Fadlullah, Z. M., Lin, X. and Kato, N. 2011. A clique-based secure admission control scheme for mobile ad hoc networks (MANETs). Journal of Network and Computer Applications 34 (6): 1827–1835.

Climent, S., Sanchez, A., Capella, J. V., Meratnia, N. and Serrano, J. J. 2014. Underwater acoustic wireless sensor networks: advances and future trends in physical, MAC and routing layers. Sensors14 (1): 795–833.

Dhurandher, S. K., Woungang, I., Gupta, A. and Bhargava, B. K. 2012. E2siw: An energy efficient scheme immune to wormhole attacks in wireless ad hoc networks. In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on , 472–477. IEEE, Fukuoka, Japan.

Djenouri, D., Mahmoudi, O., Bouamama, M., Llewellyn-Jones, D. and Merabti, M. 2007. On securing manet routing protocol against control packet dropping. In Pervasive Services, IEEE International Conference on, 100–108. IEEE, Istanbul, Turkey.

Farooq, N., Zahoor, I. and Mandal, S. 2014. Recovering from In-Band Wormhole Based Denial of Service in Wireless Sensor Networks .

Ghosh, U. and Datta, R. 2011. A secure dynamic IP configuration scheme for mobile ad hoc networks. Ad Hoc Networks 9 (7): 1327–1342.

Goyal, S. and Rohil, H. 2013. Securing MANET against Wormhole Attack using Neighbor Node Analysis. International Journal of Computer Applications .

Gupta, P. and Moudgil, S. 2014. A Novel Scheme to Detect Wormhole Attacks in Wireless Mesh Network. International Journal of Computer Science & Information Technologies 5 (3).

Hu, L. and Evans, D. 2004. Using Directional Antennas to Prevent Wormhole Attacks. In NDSS. San Diego, California.

Hwang, R.-H., Wang, C.-Y., Wu, C.-J. and Chen, G.-N. 2013. A novel efficient power-saving MAC protocol for multi-hop MANETs. International Journal of Communication Systems.

Jain, S. and Baras, J. S. 2012. Preventing wormhole attacks using physical layer authentication. In Wireless Communications and Networking Conference (WCNC), 2012 IEEE , 2712–2717. IEEE, Shanghai, China.

Jakobsen, M. K., Madsen, J. and Hansen, M. R. 2010. DEHAR: A distributed energy harvesting aware routing algorithm for ad-hoc multi-hop wireless sensor networks. In World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a , 1–9. IEEE, Montreal, QC, Canada.

Jen, S.-M., Laih, C.-S. and Kuo, W.-C. 2009. A hop-count analysis scheme for avoiding wormhole attacks in MANET. Sensors 9 (6): 5022–5039.

Jing, Y., Wang, X., Zhang, L. and Zhang, G. 2011. Stable Topology Support for Tracing DDoS Attackers in MANET. In Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE, 1–6. IEEE, Houston, TX, USA.

Keerthi, T. D. S. and Venkataram, P. 2012. Locating the attacker of wormhole attack by using the honeypot. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 1175–1180. IEEE, Liverpool, England.

Khainwar, R. S., Jain, A. and Tyagi, J. P. 2013. Elimination of Wormhole Attacker node in MANET using performance evaluation multipath algorithm. Network and Complex Systems 3 (7): 22–29.

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.

Khalil, I., Bagchi, S. and Shroff, N. B. 2008. MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks. Ad Hoc Networks 6 (3): 344–362.

Khan, Z. A. and Islam, M. H. 2012. Wormhole Attack: A new detection technique. In Emerging Technologies (ICET), 2012 International Conference on, 1–6. IEEE, Islamabad, Pakistan.

Khandare, P. and Kulkarni, N. 2013. Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack. India International Journal Of Computer Trends And Technology 4 (3): 247–252.

Khurana, S. and Gupta, N. 2011. End-to-end protocol to secure ad hoc networks against wormhole attacks. Security and Communication Networks 4 (9): 994–1002.

Krishna, S., Prasad, P., Ramanath, M. and Kumari, B. M. 2015. Security in MANET routing tables with FMNK cryptography model. In Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on.

Lathies Bhasker, T. 2013. A SCOPE FOR MANET ROUTING AND SECURITY THREATS. Economy of Industry 4 (4).

Lee, P., Clark, A., Bushnell, L. and Poovendran, R. 2013. A passivity framework for modeling and mitigating wormhole attacks on networked control systems. IEEE Transactions on 59 (12): 3224–3237.

Lego, K. and Sutradhar, D. 2011. Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Adhoc NETwork 1. Citeseer .

Li, S. and Zhu, Y. 2012. Study design of water and nitrogen optimal management model based on wireless sensor and maize growth model. In Information Science and Service Science and Data Mining (ISSDM), 2012 6th International Conference on New Trends in, 278–282. IEEE.

Liu, J., Liu, X., Jiang, X. and Sha, M. 2014. Wormhole Detection Algorithm Based on RTT and Neighborhood Information. In Proceedings of International Conference on Computer Science and Information Technology 139–145.

Lu, S., Li, L., Lam, K.-Y. and Jia, L. 2009. SAODV: a MANET routing protocol that can withstand black hole attack. In Computational Intelligence and Security, 2009. CIS'09. International Conference on, 421–425. IEEE, Beijing, China.

Maheshwari, R., Gao, J. and Das, S. R. 2007. Detecting wormhole attacks in wireless networks using connectivity information. In INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE, 107–115. IEEE, Anchorage, AK.

Malhotra, A., Bhardwaj, D. and Garg, A. 2012. Wormhole attack prevention using clustering and digital signatures in reactive routing. In Networking, Sensing and Control (ICNSC), 2012 9th IEEE International Conference on, 122–126. IEEE.

Meghdadi, M., Ozdemir, S. and Güler, I. 2011. A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. IETE Technical Review 28 (2): 89–102.

Mishra, M. A. M. and Singh, M. C. 2014. Worm-Hole Detection Mechanism for Reactive Routing of Mobile Ad-Hoc Network. International Journal of Emerging Research in Management &Technology.

Modirkhazeni, A., Aghamahmoodi, S. and Niknejad, N. 2011. Distributed approach to mitigate wormhole attack in wireless sensor networks. In Networked Computing (INC), 2011 The 7th International Conference on, 122–128. IEEE.

Modirkhazeni, A., Ithnin, N., Kadhum, M. M. and Mantoro, T. 2012. Mitigation of Wormhole Attack in Wireless Sensor Networks. Trustworthy Ubiquitous Computing 109–147.

Naiat-Abdesselam, F., Bensaou, B. and Taleb, T. 2008. Detecting and avoiding wormhole attacks in wireless ad hoc networks. Communications Magazine, IEEE 46 (4): 127–133.

Nouri, M. and Aghdam, S. A. 2011. Collaborative techniques for detecting wormhole attack in MANETs. In Research and Innovation in Information Systems (ICRIIS), 2011 International Conference on, 1–6. IEEE, Kuala Lumpur, Malaysia.

Oluoch, J., Fu, H., Younang, A., Zhu, Y. and Tri-Tran, B. 2012. A simulation study of impacts of collaborative worm hole attacks in mobile ad hoc networks (MANETs). In Proceedings of the 2012 Information Security Curriculum Development Conference, 40–45. ACM, New York, NY, USA.

Pahal, V. and Kumar, S. 2012. A Cryptographic Handshaking Approach to Prevent Worm Hole Attack in MANET. International Journal of Computer Applications 50 (2): 27–33.

Patil, V., Fulare, P. and Ghodichor, N. 2014. An Unobservable Secure Routing Protocol with Wormhole Attack Prevention for Mobile Ad-Hoc Network. International Journal of Current Engineering and Technology 4 (3): 1930–1935.

Poturalski, M., Papadimitratos, P. and Hubaux, J.-P. 2008. Secure neighbor discovery in wireless networks: formal investigation of possibility. In Proceedings of the 2008 ACM symposium on Information, computer and communications security, 189–200. ACM, New York, NY, USA.

Rahman, M. A., Anwar, F., Naeem, J. and Abedin, M. S. M. 2010. A simulation based performance comparison of routing protocol on Mobile Ad-hoc Network (proactive, reactive and hybrid). In Computer and Communication Engineering (ICCCE), 2010 International Conference on, 1–5. IEEE, Kuala Lumpur, Malaysia.

Raja, K. N. and Beno, M. M. 2014. On securing Wireless Sensor Network-Novel authentication scheme against DOS attacks. Journal of medical systems 38 (10): 1–5.

Raju, V. K. and Kumar, K. V. 2012. A simple and efficient mechanism to detect and avoid wormhole attacks in mobile ad hoc networks. In Computing Sciences (ICCS), 2012 International Conference on, 271–275. IEEE, Phagwara, India.

Roy, D. B., Chaki, R. and Chaki, N. 2010. A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks. arXiv preprint arXiv:1004.0587 .

Safi, S. M., Movaghar, A. and Mohammadizadeh, M. 2009. A novel approach for avoiding wormhole attacks in VANET. In Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on, 1–6. IEEE.

Sakthivel, T. and Chandrasekaran, R. 2012. Detection and prevention of wormhole attacks in MANETs using path tracing approach. European Journal of Scienti c Research 76 (2): 240–252.

Sandeep, J. and Kumar, J. S. 2015. Efficient Packet Transmission and Energy Optimization in Military Operation Scenarios of MANET. Procedia Computer Science47: 400–407.

Satheeshkumar, M. B. and Kalaivani, M. R. 2014. Privacy Protection Against Wormhole Attacks In Manet. tra c 2 (1).

Sawhney, R. and Vohra, R. 2012. Physical Characteristics based MANET Routing Protocols for Campus Network. International Journal of Computer Applications 48 (3): 1851–1856.

Shah, V. and Modi, N. 2014. Responsive Parameter based an AntiWorm Approach to Prevent Wormhole Attack in Ad hoc Networks .

Shamaei, S. and Movaghar, A. 2015. A Two-Phase Wormhole Attack Detection Scheme in MANETs. The ISC International Journal of Information Security 6 (2).

Sharma, S. and Singh, T. 2013. An effective intrusion detection system for detection and correction of gray hole attack in MANETs. International journal of computer applications (0975-8887, volume 68-No. 12

Shi, F., Liu, W., Jin, D. and Song, J. 2013. A countermeasure against wormhole attacks in MANETs using analytical hierarchy process methodology. Electronic Commerce Research13 (3): 329–345.

Smys, S. and Bala, G. J. 2012. Efficient self-organized backbone formation in mobile ad hoc networks (MANETs). Computers & Electrical Engineering 38 (3): 522–532.

Stoleru, R., Wu, H. and Chenji, H. 2012. Secure neighbor discovery and wormhole localization in mobile ad hoc networks. Ad Hoc Networks 10 (7): 1179–1190.

Su, M.-Y. 2010. WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. computers & security 29 (2): 208–224.

Sudarsan, M. S., Vinodhini, M. and Karthik, S. 2012. Enhancing Key Management In Intrusion Detection System For Manets. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1 (8): pp–219.

Sun, B., Gui, C. and Liu, P. 2010. Energy Entropy Multipath Routing optimization algorithm in MANET based on GA. In Bio-Inspired Computing: Theories and Applications (BIC-TA), 2010 IEEE Fifth International Conference on, 943–947. IEEE, Changsha, China.

Upadhyay, S. and Bajpai, A. 2012. Avoiding Wormhole attack in MANET using statistical analysis approach. International Journal on Cryptography and Information Security .

Vani, A. and Rao, D. S. 2011. A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks. International Journal on Computer Science and Engineering (IJCSE) 3 (6): 2377–2384.

Venkataraman, R., Pushpalatha, M., Rao, T. R. and Khemka, R. 2009. A graphtheoretic algorithm for detection of multiple wormhole attacks in mobile ad hoc networks. International Journal of Recent Trends in Engineering (IJRTE) 1 (2): 220–222.

Vijayalakshmi, S. and Albert Rabara, S. 2011. Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques-LP3 and NAWA2 .

Viswanathan, M. 2013. An Unobservable Secure Path Tracing Routing Protocol For Mobile Adhoc Networks. In International Journal of Engineering Research and TechnologyESRSA Publications.

Wang, B., Chen, X. and Chang, W. 2014. A light-weight trust-based QoS routing algorithm for ad hoc networks. Pervasive and Mobile Computing13: 164–180.

Zhang, Y. and Feng, X. 2012, In Recent Advances in Computer Science and Information Engineering, In Recent Advances in Computer Science and Information Engineering , 195–201, Springer, 195–201.

Zhang, Y., Yan, T., Tian, J., Hu, Q., Wang, G. and Li, Z. 2014. TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks. Ad Hoc Networks 21 (5): 109–122.

Zhao, J. and Nygard, K. E. 2011. A Two-Phase Security Algorithm for Hierarchical Sensor Networks. In FUTURE COMPUTING 2011, The Third International Conference on Future Computational Technologies and Applications, 114–120. Rome, Italy.

Znaidi, W., Minier, M. and Babau, J.-P. 2008. Detecting wormhole attacks in wireless networks using local neighborhood information. In Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on, 1–5. IEEE.