UNIVERSITI PUTRA MALAYSIA

DETECTION OF BLACK HOLE NODES IN MOBILE AD HOC NETWORK USING HYBRID TRUSTWORTHINESS AND ENERGY CONSUMPTION TECHNIQUES

AHMED SUDAD MUSTAFA

FK 2017 12

DETECTION OF BLACK HOLE NODES IN MOBILE AD HOC NETWORK USING HYBRID TRUSTWORTHINESS AND ENERGY CONSUMPTION TECHNIQUES

By

AHMED SUDAD MUSTAFA

Thesis submitted to the School of Graduate Studies, Universiti Putra Malaysia in fulfillment of the requirements for the degree of Master of Science

March 2017

© COPYRIGHT UPM

© COPYRIGHT UPM

COPYRIGHT

All material contained within the thesis, including without limitation, texts, logos, icons, photographs, and all other artwork, is copyright material of University Putra Malaysia unless otherwise stated. Use may be made of any material contained within the thesis for non-commercial purposes from copyright holder. Commercial use of material may only be made with express, prior, written permission of Universiti Putra Malaysia.

Copyright© Universiti Putra Malaysia

© COPYRIGHT UPM

DEDICATION

This thesis is dedicated to

All those I love

Especially

My dearest parents

My brothers and sister

For their endless encouragement, patience, and support and for being a great source of motivation and inspiration

And to all my friends

© COPYRIGHT UPM

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

DETECTION OF BLACK HOLE NODES IN MOBILE AD HOC NETWORK USING HYBRID TRUSTWORTHINESS AND ENERGY CONSUMPTION TECHNIQUES

By

AHMED SUDAD MUSTAFA

March 2017

Chairman : Sharifah Mumtazah Syed Ahmad, PhD
Faculty : Engineering

Mobile ad-hoc network (MANET) is an evolving technology that is utilized in different applications (i.e. military surveillance, personal network, etc.) and developed in the recent years. Nodes in MANET are capable of functioning as a router for data communication. MANET devices do not require central management, capable of self-organizing/ healing through persistent reconfiguration. Any MANET node requires a protocol in order to communicate with its neighbor within its transmission range.

Ad hoc on-demand distance vector routing protocol (AODV) is a commonly used protocol in MANET. AODV is a reactive protocol that offers relatively low routing overhead since the nodes utilizing this protocol operates only when a route is requested. However, AODV suffers severely from the black hole attacks where the attacker node advertise itself as having the optimum path leading to the destination node by varying some essential parameters. Therefore, detecting the black hole in the network is substantial since MANET depends on the cooperation between adjacent nodes. In this thesis, a hybrid detection algorithm mechanism has been proposed which combines two detection algorithms based on nodes' trustworthiness and energy consumption in a parallel manner in order to detect the black hole nodes. An empirical testing approach was utilized here where several scenarios have been implemented and investigated in order to find the optimal settings. Network simulator (NS2) simulation findings demonstrate that the trust based algorithm achieves an average packet delivery ratio (PDR) of 87.3%, end to end delay (EED) of 7.47 ms and black hole detection accuracy of 90%. On the other hand, the detection algorithm based on the energy consumption achieves PDR of 91.6%, EED of 14.03 ms and detection rate accuracy of 93%. The hybrid technique offers decent average PDR of 94.7, EED of 8.62 ms and improved black hole detection rate

© COPYRIGHT UPM

accuracy of 96%. Furthermore, the hybrid technique offers reduced end to end delay with relatively high PDR when compared with two recent works.

© COPYRIGHT UPM

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

PENGESANAN BLACK HOLE NOD DI MOBILE AD HOC NETEORK MENGGUNAKAN AMANAH DAN TENAGA TEKNIK PENGGUNAAN HIBRID

Oleh

AHMED SUDAD MUSTAFA

Mac 2017

Pengerusi : Sharifah Mumtazah Syed Ahmad, PhD
Fakulti : Kejuruteraan

Rangkaian ad-hoc mudah alih (MANET) merupakan sesuatu teknologi yang berkembang yang digunakan dalam pelbagai aplikasi (seperti pengawasan tentera, rangkaian peribadi, dan lain-lain) dan telah dibangunkan sejak kebelakangan ini. Nod di dalam MANET berkemampuan untuk berfungsi sebagai penghala bagi komunikasi data. Peralatan MANET tidak memerlukan pengurusan pusat dan berkemampuan untuk menguruskan / penyembuhan diri melalui konfigurasi yang berterusan. Sebarang nod MANET memerlukan protokol untuk berkomunikasi dengan jirannya dalam jarak penghantaran tersebut.

Protokol penghalaan ad-hoc atas permintaan jarak vektor (AODV) adalah protokol yag sering digunakan dalam MANET. AODV merupakan protokol reaktif yang menawarkan overhead penghalaan yang rendah kerana nod-nod tyang menggunakan protokol ini beroperasi hanya apabila laluan diminta. Walau bagaimanapun, AODV terjejas teruk akibat dari serangan lubang hitam dimana nod penyerang mengiklankan dirinya sebagai mempunyai laluan yang optimum untuk ke nod destinasi dengan mengubah beberapa parameter yang penting. Oleh itu, pengesanan lubang hitam di dalam rangkaian adalah penting kerana MANET bergantung kepada kerjasama di antara nod-nod bersebelahan. Dalam tesis ini, sebuah algoritma pengesanan hibrid telah dicadangkan yang menggabungkan dua algoritma pengesanan berdasarkan kebolehpercayaan nod dan penggunaan tenaga dengan cara yang selarian untuk mengesab nod-nod lubang hitam. Sebuah pendekatan ujian empirikal telah digunakan di sini di mana beberapa senario telah dilaksanakan dan disiasat untuk mendapatkan tetapan-tetapan yang optimum. Hasil simulasi rangkaian simulator (NS2) menunjukkan bahawa algoritma berdasarkan kebolehpercayaan telah mencapai nisbah purata penghantaran paket (PDR) sebanyak 87.3%, tempoh kelewatan hujung ke hujung (EED) sebanyak 7.47 mili saat dan ketepatan pengesanan nod lubang hitam sebanyak 90%. Pada masa yang sama, algoritma

© COPYRIGHT UPM

bersadarkan menggunaan tenaga telah mencapai PDR sebanyak 91.6%, EER sebanyak 14.03 mili saaat dan ketepatan pengesanan nod lubang hitam sebanyak 93%. Tambahan pula, teknik hibrid menawarkan pengurangan tempoh kelewatan hujung ke hujung dengan PDR yang agak tinggi sedikit apabila dibandingkan dengan dua kerja penyelidikan yang terkini.

© COPYRIGHT UPM

ACKNOWLEDGEMENT

First of all, I would like to express my gratitude to my supervisor, Dr. Sharifah Mumtazah Syed Ahmad for her continuous support, invaluable guidance, and patience as well as her encouragement and inspiration along this research journey without which, this thesis could not be done as smoothly as what we have. I am very thankful for all the tasks she has produced for me. God bless her and her family.

Deep gratitude also goes to my co-supervisor Dr. Fazirulhisyam Hashim for his helpful guidance on the thesis draft helped improve the quality of this work. God bless her and her family.

Besides, to my dear friends and peers, I am so grateful to have companions like you by my side during this trip to pursue my degree. It is you who let me feel warm all the time to make my life abroad complete and colorful.

Most importantly, I want to say thanks to my dearest parents and my brothers and sister. They helped me out during the difficulties in life and provided me with warm encouragement.

© COPYRIGHT UPM

I certify that a Thesis Examination Committee has met on 30 March 2017 to conduct the final examination of Ahmed Sudad Mustafa Mustafa on his thesis entitled "Detection of Black Hole Nodes in Mobile Ad Hoc Network using Hybrid Trustworthiness and Energy Consumption Techniques" 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:

Khairulmizam bin Samsudin, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Shaiful Jahari bin Hashim, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Salman bin Yussof, PhD
Associate Professor
Universiti Tenaga Nasional
Malaysia
(External Examiner)

NOR AINI AB. SHUKOR, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 28 April 2017

This thesis was submitted to the senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the supervisory committee were as follows:

Sharifah Mumtazah Syed Ahmad, PhD
Associate. Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Fazirulhisyam Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

ROBIAH BINTI YUNUS, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

© COPYRIGHT UPM

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institution;
- 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 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 Matriculation No.: Ahmed Sudad Mustafa, GS42799

© COPYRIGHT UPM

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) were adhered to.

Signature: _____
Name of Chairman of Supervisory Committee: Associate. Professor Dr. Sharifah Mumtazah Syed Ahmad

Signature: _____
Name of Member of Supervisory Committee: Dr. Fazirulhisyam Hashim

© COPYRIGHT UPM

TABLE OF CONTENTS

© COPYRIGHT UPM

© COPYRIGHT UPM

LIST OF TABLES

© COPYRIGHT UPM

LIST OF FIGURES

© COPYRIGHT UPM

© COPYRIGHT UPM

LIST OF ABBREVIATIONS

ACO	Ant Colony Optimization
AODV	Ad hoc On-Demand Distance Vector
ARA	Ant Colony Based Routing Algorithm
ARQ	automatic repeat request
AUC	Area under the curve
BH	Black hole
CBR	constant bit rate
CMT	cable mode transition
DoS	Denial of Service
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing Protocol
E	Energy
EED	End-to-end Delay
FEC	forward error correction
FN	false negative
FPR	False positive ratio
GPS	Global positioning system
IN	Intermediate node
LN	Leader node
MAC	media access control
MANET	Mobile ad hoc network
MID	Multiple Interface Declaration
MPR	Multi-Point Distribution Relays
NS	Network Simulator
OLSR	Optimized Link State Routing Protocol
OSI	Open Systems Interconnection
PD	Processing Delay
PDR	Packet Delivery Ratio
PT	Propagation Time
QT	Queuing Time
RERR	Route Error
ROC	Receiver Operating Characteristic

© COPYRIGHT UPM

RREP	Route Reply
RREQ	Route Request
SAODV	Secured Ad Hoc On-Demand Distance Vector
T	Threshold
TC	Topology Control
THe	Energy Threshold
THw	Trust Threshold
TI	Timer
TN	True Negative
TPR	True Positive Rate
TR	Transmission Range
TT	Transmission Time
TTL	Time to Live
TW	Trust Weight
ZRP	Zone Routing Protocol

© COPYRIGHT UPM

CHAPTER 1

INTRODUCTION

1.1 Background

Mobile ad hoc network (MANET) is a combination of nodes that are moveable and has a dynamic topology in nature. It basically represents a sophisticated distributed system that is formed by a group of wireless mobile nodes, which communicate using wireless medium. The MANET nodes capable of operating as router for data communication within the grid. Due to the unique characteristics of MANET such as low cost as well as mobility, MANET is adequate for wide variety of applications such as monitoring and detecting specific events, battlefield surveillance, flood detection, health care, and home applications [1-6].

Routing is the main concern in MANET, since it is susceptible to error due to the mobility of the nodes as well as its dynamic topology. Earlier researchers focused on the efficiency of route establishment, so they considered all of the nodes are trustworthy [7, 8]. However, this scenario has been challenged recently as more attacks emerged to threaten MANET security [9].

Fundamentally, any MANET topology utilizes a communication protocol in order to operate such as Ad hoc On-Demand Distance Vector (AODV) and Destination-Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR). Each one of these protocols has its own advantages and flaws [10]. However, AODV offers less packet loss and decent average delay as compared to the other protocols [11]. Thus, it is one of the most common routing protocols within MANET. AODV is a power efficient protocol since it does not rely on active links neither preserve any routing information. Furthermore, nodes do not have to discover or preserve a path to another node unless the two nodes require data transformation [12].

Whenever a specific node needs to send data to a destination node, a route discovery procedure is initiated by broadcasting a packet called route request (RREQ) to all its neighbors. Whenever an intermediate node has a fresh path to the destination, it immediately sends back a packet called route reply (RREP) to the source. In case a disconnect occurs between the two nodes, a route error (RERR) message is being sent indicating a disconnect in the route. Despite the advantages of AODV [7], it is vulnerable to the black hole attack, since it does not feature any defensive mechanism [8]. AODV protocol uses the sequence number as well as hop-count in order to determine the best route for data transmission. The higher sequence number means a better route for communication. The black hole node uses this property in order to lure the source to send the actual data to it by sending a bogus reply message carrying very high sequence number and low hop-count.

Basically, the black hole attack has two phases. The first one, the black hole node exploits the AODV routing protocol to declare itself as having a proper path to the destination node by increasing the sequence number as well as decreasing the hop count field. The second phase is when the black hole node drop every single packet it receives from the source node [13]. Eventually, the whole network will collapse.

1.2 Problem Statement

Black hole attacks in MANET have been a major issue for the past few years [10]. Any MANET network utilizes a specific routing protocol in order to send/ receive data packets, whether it is a reactive or a proactive protocol. Black hole attacks normally exploit the AODV protocol in order to perform its malicious activities. Since, ADOV does not have a concrete mechanism to fight the black hole attacks. Thus, researchers have proposed different types of approaches to remedy this issue. One of which includes a trust-based approach, by initiating a trust weight for all the nodes and keep monitoring the nodes using leader nodes with higher privilege (i.e. nodes capable of insolating specific nodes if necessary), or a cooperative approach by enabling the nodes to listen to each other. This involves detecting the node which its trust weight falls below the predefined threshold value [12]. Such approaches are decent with regards to the malicious detection rate. However, it offers relatively high average delay.

Other researchers used anomaly-based intrusion detection system (IDS) in order to isolate the black hole nodes in AODV [13]. This approach operates by implementing a baseline procedure for the network to operate. This procedure will include all the genuine activities that can be done in the normal circumstances and isolate any activity that falls outside the procedure. This approach offers a decent average delay. However, it suffers from the high false positive.

Our approach involves combining two fundamental algorithms. The first algorithm is based on trust technique that offers decent detection accuracy with minimal delay. Our hypothesis is that the detection accuracy can be further improved if another algorithm is added as a second layer of protection. The assumption is that, the second algorithm will not incur a heavy computational process that could burden the system. The second algorithm is based on the initial energy consumption of the nodes to locate the black hole node and detect it. The main aim of this research is to further improve the detection rate accuracy of malicious nodes and achieving higher packet delivery ratio (PDR) as well via the hybrid algorithm.

© COPYRIGHT UPM

1.3 Research Aim and Objectives

1. To design and develop detection algorithm based on the trustworthiness among the AODV nodes in order to detect the black hole nodes.
2. To design and develop detection algorithm based on the initial energy consumption of the nodes in order to detect the black hole nodes within the AODV.
3. To combine the two approaches in order to enhance the PDR and black hole detection rate.

1.4 Thesis Scope

The scope of this research focuses solely on the internal-passive black hole attacks that can be launched against the AODV routing protocol by intruders. The internal black hole attack is difficult to detect since the attacker impersonates an existing node within the network to perform any malicious activity. This research considers the scenario where all the nodes in the topology are movable. This research also features receiver operating characteristic (ROC) curves that provide a comprehensive analysis in terms of malicious node detection rate. Furthermore, this research also seeks to offer an investigation of optimal scenario where minimal end to end delay is being produced as well as improved PDR. The proposed algorithms will assume the following:

The proposed algorithms are based on the following assumptions:

1. All leader nodes are trustworthy.
2. The two implemented black hole nodes are internal and passive type.
3. The black hole nodes are in a strategic position that allows them to participate in most network traffics.
4. The proposed algorithms are applied after the route discovery phase
5. The leader nodes are able to sniff all routing packets within their transmission range even if the packets are not intended for them using the promiscuous mode.
6. The black hole nodes ID are broadcasted successfully.
7. The leader nodes do not participate in the data transmission.
8. All node IDs are unique.

© COPYRIGHT UPM

1.5 Motivation

Security of mobile ad hoc network (MANET) is one of the most difficult challenges. This is mainly because of the natural behavior of MANET such as open wireless medium, node mobility, bounded processing power, shortage of central monitoring, lack of obvious defensive technique and availability of the consumable resources such as bandwidth and battery power.

In order to assure a secure transmission over MANET, a comprehensive overview of different types of security threats and their effects is required. Black hole attack, wormhole attack, Sybil attack, routing table overflow attack, flooding attack, selfish node misbehavior, Denial of Service attack (DoS) and impersonating attack are the types of attacks that can be triggered against MANETs. A detailed explanation of possible hostile attack on MANET is discussed in [14] literature.

Generally, MANET is more susceptible to these kinds of attacks since one node in the MANET will assume all the nodes in the neighborhood are trustworthy [7]. MANET suffers not only from same types of threats like DoS and message distortion, IP spoofing as the infrastructure network. However, it also suffers from new threats caused by the exclusive characteristics of MANET like wormhole attack and black hole attack. For instance, black hole attack occurs when one node in the network advertise itself as having the best route from the source to the destination. This gives the malicious node the capability to insert itself in between the communicating nodes. Consequently, the malicious node drops all the packets it receives. MANET is more vulnerable to such unique attacks since the transmission is based on the common trust among participating nodes. In addition, there is no centralized monitoring of any misbehavior node.

The outcome of the research on securing the MANET against black hole attacks are the methods that either needs promiscuous monitoring to MANET nodes or incur considerable computational sophistication in individual nodes which eventually depletes their confined resources such as bandwidth, memory and power. Therefore, the main objective of this dissertation is to detect the black hole nodes that exist in MANET by proposing a new hybrid technique that can detect the black hole attacks efficiently with high PDR and better detection rate of black hole nodes.

© COPYRIGHT UPM

1.6 Thesis Organization

This dissertation shows how the black hole attacks in MANET can be detected efficiently. The organization of this thesis is as follows. Chapter 2 introduces the literature review. We first provide a broad overview regarding mobile ad hoc network. Then we describe in detail MANET architecture and its corresponding layers. Then we talk about the structure of MANET and its different possible applications. Next, we introduce MANET routing tables and their classifications. Next, we describe the security threats in MANET and its flaws. Then, we explain the black hole attack in details and how it is devastating against AODV protocol. Last but not least in chapter 2, we introduce the related work models, and show how our work is distinguished from the others. Chapter 3 introduce our methodology to detect the black hole attack nodes. Here, we design a trust based intrusion detection system and test it. Then, we design another intrusion detection system based on the initial energy consumption and test it. Next, we combine both algorithms in order to enhance the malicious nodes detection rate and PDR. In chapter 4 we include our results and analysis with the proper diagrams. Chapter 5 presents our conclusion as well as proposed future work.

© COPYRIGHT UPM

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *Communications magazine, IEEE,* vol. 40, no. 8, pp. 102-114, 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer networks,* vol. 52, no. 12, pp. 2292-2330, 2008.

[3] A. Boukerche, *Algorithms and protocols for wireless, mobile Ad Hoc networks*. John Wiley & Sons, 2008.

[4] K. Sohraby, D. Minoli, and T. Znati, *Wireless sensor networks: technology, protocols, and applications*. John Wiley & Sons, 2007.

[5] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors,* vol. 9, no. 9, pp. 6869-6896, 2009.

[6] C. E. Perkins, *Ad hoc networking*. Addison-wesley Reading, 2001.

[7] J.-H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials,* vol. 13, no. 4, pp. 562-583, 2011.

[8] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE,* vol. 98, no. 10, pp. 1755-1772, 2010.

[9] H. L. Nguyen and U. T. Nguyen, "A study of different types of attacks on multicast in mobile ad hoc networks," *Ad Hoc Networks,* vol. 6, no. 1, pp. 32-46, 2008.

[10] D. O. Jorg, "Performance comparison of MANET routing protocols in different network sizes," *Computer Networks & Distributed Systems,* 2003.

[11] N. S. M. Usop, A. Abdullah, and A. F. A. Abidin, "Performance evaluation of AODV, DSDV & DSR routing protocol in grid environment," *IJCSNS International Journal of Computer Science and Network Security,* vol. 9, no. 7, pp. 261-268, 2009.

[12] H. Kaur, V. Sahni, and M. Bala, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review," 2013, *network,* vol. 10, p. 11.

[13] E. S. Kaur and E. B. Singh, "A Survey on Black Hole Attack on AODV Routing Protocol in Wireless Adhoc Networks," in *International Journal of*

© COPYRIGHT UPM

Engineering Research and Technology, 2013, vol. 2, no. 8 (August-2013): ESRSA Publications.

[14] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, "Different types of attacks on integrated MANET-Internet communication," *International Journal of Computer Science and Security*, vol. 4, no. 3, pp. 265-274, 2010.

[15] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks," *Ad hoc networks*, vol. 3, no. 3, pp. 325-349, 2005.

[16] M. A. Labrador and P. M. Wightman, *Topology Control in Wireless Sensor Networks: with a companion simulation tool for teaching and research*. Springer Science & Business Media, 2009.

[17] M. Matin and M. Islam, *Overview of wireless sensor network*. INTECH Open Access Publisher, 2012.

[18] C.-T. Cheng, C. K. Tse, and F. Lau, "A delay-aware data collection network structure for wireless sensor networks," *Sensors Journal, IEEE*, vol. 11, no. 3, pp. 699-710, 2011.

[19] B. Paul and M. A. Matin, "Optimal geometrical sink location estimation for two-tiered wireless sensor networks," *Wireless Sensor Systems, IET*, vol. 1, no. 2, pp. 74-84, 2011.

[20] F. Fabbri, J. Riihijärvi, C. Buratti, R. Verdone, and P. Mähönen, "Area throughput and energy consumption for clustered wireless sensor networks," in *WCNC*, 2009, pp. 2468-2473: Citeseer.

[21] X. Han, X. Cao, E. L. Lloyd, and C.-C. Shen, "Fault-tolerant relay node placement in heterogeneous wireless sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 5, pp. 643-656, 2010.

[22] W. Liu, C. Zhang, G. Yao, and Y. Fang, "DELAR: a device-energy-load aware relaying framework for heterogeneous mobile ad hoc networks," *IEEE journal on selected areas in communications*, vol. 29, no. 8, pp. 1572-1584, 2011.

[23] F. H. Fitzek and M. D. Katz, *Cooperation in wireless networks: principles and applications*. Springer, 2006.

[24] A. A. A. Alkhatib and G. S. Baicher, "Wireless sensor network architecture," in *2012 International Conference on Computer Networks and Communication Systems (CNCS 2012)*, 2012.

[25] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393-422, 2002.

[26] A. Baadache and A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," *arXiv preprint arXiv:1002.1681*, 2010.

© COPYRIGHT UPM

[27] A. Koubâa, M. Alves, and E. Tovar, "Lower protocol layers for wireless sensor networks: a survey," 2005.

[28] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC essentials for wireless sensor networks," *Communications Surveys & Tutorials, IEEE,* vol. 12, no. 2, pp. 222-248, 2010.

[29] G. Meghan and G. Simon, "A comparative study of medium access control protocols for wireless sensor networks," *Int'l J. of Communications, Network and System Sciences,* vol. 2, no. 08, p. 695, 2009.

[30] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer networks,* vol. 51, no. 4, pp. 921-960, 2007.

[31] P. R. Pereira *et al.*, "End-to-end reliability in wireless sensor networks: Survey and research challenges," in *EuroFGI Workshop on IP QoS and Traffic Control*, 2007, vol. 54, pp. 67-74.

[32] H. Atwell, D. J. McManus, and H. H. Carr, "The OSI Model and the Seven Chakras of Hinduism: A Comparative Analysis," *International Journal of Applied,* vol. 3, no. 3, 2013.

[33] C. Tschudin, P. Gunningberg, H. Lundgren, and E. Nordström, "Lessons from experimental MANET research," *Ad Hoc Networks,* vol. 3, no. 2, pp. 221-233, 2005.

[34] J. S. Wilson, *Sensor technology handbook*. Elsevier, 2004.

[35] I. Aaronson and P. A. Worfolk, "Communications protocol for packet data particularly in mesh topology wireless networks," ed: Google Patents, 2002.

[36] S. M. Faccin, C. Wijting, J. Kenckt, and A. Damle, "Mesh WLAN networks: concept and system design," *Wireless Communications, IEEE,* vol. 13, no. 2, pp. 10-17, 2006.

[37] W. Lee and G. E. Sobelman, "Mesh-star hybrid noc architecture with cdma switch," in *2009 IEEE International Symposium on Circuits and Systems*, 2009, pp. 1349-1352: IEEE.

[38] W. Lee and G. E. Sobelman, "Mesh-star hybrid noc architecture with cdma switch," in *Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on*, 2009, pp. 1349-1352: IEEE.

[39] W. C. Craig, "Zigbee: wireless control that simply works," *ZigBee Alliance* http://www. *zigbee. org/resources/documents/2004_Zig Bee_CDC-P810_Craig_Paper. pdf*, 2004.

[40] N. Xu, "A survey of sensor network applications," *IEEE Communications Magazine,* vol. 40, no. 8, pp. 102-114, 2002.

© COPYRIGHT UPM

[41] W. B. Heinzelman, A. L. Murphy, H. S. Carvalho, and M. A. Perillo, "Middleware to support sensor network applications," *Network, IEEE,* vol. 18, no. 1, pp. 6-14, 2004.

[42] H. Frey, S. Rührup, and I. Stojmenović, "Routing in wireless sensor networks," in *Guide to Wireless Sensor Networks*: Springer, 2009, pp. 81-111.

[43] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," 2070-1721, 2003.

[44] C. Mbarushimana and A. Shahrabi, "Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks," in *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on*, 2007, vol. 2, pp. 679-684: IEEE.

[45] S. R. Das, E. M. Belding-Royer, and C. E. Perkins, "Ad hoc on-demand distance vector (AODV) routing," 2003.

[46] I. D. Chakeres and E. M. Belding-Royer, "AODV routing protocol implementation design," in *Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on*, 2004, pp. 698-703: IEEE.

[47] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *ACM SIGMOBILE Mobile Computing and Communications Review,* vol. 6, no. 3, pp. 106-107, 2002.

[48] P. K. Maurya *et al.*, "An overview of AODV routing protocol," *International Journal of Modern Engineering Research (IJMER),* vol. 2, no. 3, pp. 728-732, 2012.

[49] M. Medadian, A. Mebadi, and E. Shahri, "Combat with Black Hole attack in AODV routing protocol," in *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on*, 2009, pp. 530-535: IEEE.

[50] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile computing*: Springer, 1996, pp. 153-181.

[51] C. Zhu, M. J. Lee, and T. Saadawi, "Rtt-based optimal waiting time for best route selection in ad hoc routing protocols," in *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*, 2003, vol. 2, pp. 1054-1059: IEEE.

[52] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad hoc networks,* vol. 2, no. 1, pp. 1-22, 2004.

© COPYRIGHT UPM

[53] T. Clausen and P. Jacquet, "RFC 3626: Optimized link state routing protocol (OLSR)," *IETF, October*, vol. 4, 2003.

[54] S. Mohseni, R. Hassan, A. Patel, and R. Razali, "Comparative review study of reactive and proactive routing protocols in MANETs," in *4th IEEE International Conference on Digital Ecosystems and Technologies*, 2010, pp. 304-309: IEEE.

[55] W. Ullah, H. Ali, A. W. Khan, A. Farhad, B. Ahmad, and A. Khan, "Performance assessment of reactive routing protocols in Mobile Ad-hoc Networks under CBR traffic using NS2," in *Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on*, 2016, pp. 1026-1029: IEEE.

[56] Z. J. Haas, M. R. Pearlman, and P. Samar, "The zone routing protocol (ZRP) for ad hoc networks," 2002.

[57] J. Schaumann, "Analysis of the zone routing protocol," *Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December*, 2002.

[58] S. Sesay, Z. Yang, and J. He, "A survey on mobile ad hoc wireless network," *Information Technology Journal*, vol. 3, no. 2, pp. 168-175, 2004.

[59] K. Biswas and M. Ali, "Security threats in mobile ad hoc network," 2007.

[60] F. Xing and W. Wang, "Understanding dynamic denial of service attacks in mobile ad hoc networks," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*, 2006, pp. 1-7: IEEE.

[61] M. R. Ahmed, X. Huang, and D. Sharma, "A taxonomy of internal attacks in wireless sensor Network," *Memory (Kbytes)*, vol. 128, p. 48, 2012.

[62] P. Vinayakray-Jani, "Security within ad hoc networks," in *Proceeding of PAMPAS Workshop*, 2002.

[63] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," *Computer Communications*, vol. 34, no. 1, pp. 107-117, 2011.

[64] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, 2012, pp. 535-541: IEEE.

[65] M. Parsons and P. Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks," in *roceedings of Field Failure Data Analysis Workshop September27-30, Niagara Falls, New York, USA*, 2009.

© COPYRIGHT UPM

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

[67] N. Shanthi, L. Ganesan, and K. Ramar, "STUDY OF DIFFERENT ATTACKS ON MULTICAST MOBILE AD HOC NETWORK," *Journal of Theoretical & Applied Information Technology*, vol. 6, no. 4, 2009.

[68] A. Vani and D. S. Rao, "Providing of Secure Routing against Attacks in MANETs," *International Journal of Computer Applications (0975–8887) Volume*, 2011.

[69] H. Al Amri, M. Abolhasan, and T. Wysocki, "Scalability of MANET routing protocols for heterogeneous and homogenous networks," *Computers & Electrical Engineering*, vol. 36, no. 4, pp. 752-765, 2010.

[70] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," *Human-centric Computing and Information Sciences*, vol. 1, no. 1, pp. 1-16, 2011.

[71] C. Wei, L. Xiang, B. Yuebin, and G. Xiaopeng, "A new solution for resisting gray hole attack in mobile ad-hoc networks," in *Communications and Networking in China, 2007. CHINACOM'07. Second International Conference on*, 2007, pp. 366-370: IEEE.

[72] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET," *Karlstads University, Sweden*, 2006.

[73] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," *IJ Network Security*, vol. 5, no. 3, pp. 338-346, 2007.

[74] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *Communications Magazine, IEEE*, vol. 40, no. 10, pp. 70-75, 2002.

[75] M. Parsons and P. Ebinger, "Interaction: I. Social Interaction," in *The international encyclopedia of the social sciences*, 1968: Citeseer.

[76] S. Biswas, T. Nag, and S. Neogy, "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET," in *Applications and Innovations in Mobile Computing (AIMoC), 2014*, 2014, pp. 157-164: IEEE.

[77] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking*, 1998, pp. 85-97: ACM.

© COPYRIGHT UPM

[78] A. Dhaka, A. Nandal, and R. S. Dhaka, "Gray and Black Hole Attack Identification Using Control Packets in MANETs," *Procedia Computer Science*, vol. 54, pp. 83-91, 2015.

[79] R. K. Bar, J. K. Mandal, and M. M. Singh, "QoS of MANet through trust based AODV routing protocol by exclusion of black hole attack," *Procedia Technology*, vol. 10, pp. 530-537, 2013.

[80] Y. F. Alem and Z. C. Xuan, "Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection," in *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, 2010, vol. 3, pp. V3-672-V3-676: IEEE.

[81] N. Choudhary and L. Tharani, "Preventing black hole attack in AODV using timer-based detection mechanism," in *Signal processing and communication engineering systems (SPACES), 2015 international conference on*, 2015, pp. 1-4: IEEE.

[82] N. R. Yerneni and A. K. Sarje, "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc," in *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on*, 2012, pp. 1-5: IEEE.

[83] M. R. Babu and G. Usha, "A Novel Honeypot Based Detection and Isolation Approach (NHBADI) To Detect and Isolate Black Hole Attacks in MANET," 2016, *Wireless Personal Communications*, pp. 1-15.

[84] T. Poongodi and M. Karthikeyan, "Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks," 2016, *Wireless Personal Communications*, pp. 1-12.

[85] K. Cook, "Trust in Society, vol. 2, Feb. 2003," *Russell Sage Foundation Series on Trust, New York*.

[86] P.-E. Danielsson, "Euclidean distance mapping," *Computer Graphics and image processing*, vol. 14, no. 3, pp. 227-248, 1980.

[87] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "Authenticated routing for ad hoc networks," *IEEE Journal on selected areas in communications*, vol. 23, no. 3, pp. 598-610, 2005.

[88] T. Srinivasan, V. Vijaykumar, and R. Chandrasekar, "A self-organized agent-based architecture for power-aware intrusion detection in wireless ad-hoc networks," in *2006 International Conference on Computing & Informatics*, 2006, pp. 1-6: IEEE.

[89] J.-C. Cano and P. Manzoni, "A performance comparison of energy consumption for mobile ad hoc network routing protocols," in *Modeling, Analysis and Simulation of Computer and Telecommunication Systems, 2000. Proceedings. 8th International Symposium on*, 2000, pp. 57-64: IEEE.

© COPYRIGHT UPM

[90] J. JáJá, *An introduction to parallel algorithms*. Addison-Wesley Reading, 1992.

[91] T. Issariyakul and E. Hossain, *Introduction to network simulator NS2*. Springer Science & Business Media, 2011.

[92] S. A. Jafar and A. Goldsmith, "Transmitter optimization and optimality of beamforming for multiple antenna systems," *IEEE Transactions on Wireless Communications*, vol. 3, no. 4, pp. 1165-1175, 2004.

[93] P. Rohal, R. Dahiya, and P. Dahiya, "Study and analysis of throughput, delay and packet delivery ratio in MANET for topology based routing protocols (AODV, DSR and DSDV)," *international journal for advance research in engineering and technology*, vol. 1, no. 2, pp. 54-58, 2013.

[94] R. Fotohi, S. Jamali, and F. Sarkohaki, "Performance Evaluation of AODV, LHC-AODV, OLSR, UL-OLSR, DSDV Routing Protocols," *International Journal of Information Technology and Computer Science (IJITCS)*, vol. 5, no. 10, p. 21, 2013.

[95] J. A. Hanley and B. J. McNeil, "The meaning and use of the area under a receiver operating characteristic (ROC) curve," *Radiology*, vol. 143, no. 1, pp. 29-36, 1982.

[96] L. Tamilselvan and V. Sankaranarayanan, "Prevention of blackhole attack in MANET," in *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)*, 2007, pp. 21-21: IEEE.

[97] T. Fawcett, "An introduction to ROC analysis," *Pattern recognition letters*, vol. 27, no. 8, pp. 861-874, 2006.

[98] A. P. Bradley, "The use of the area under the ROC curve in the evaluation of machine learning algorithms," *Pattern recognition*, vol. 30, no. 7, pp. 1145-1159, 1997.

[99] F. Abdel-Fattah, F. Dahalin, and S. Jusoh, "Distributed and cooperative hierarchical intrusion detection on MANETs," *International Journal of Computer Applications*, vol. 12, no. 5, 2010.

[100] A. K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile Ad hoc Networks," in *Pervasive computing (ICPC), 2015 international conference on*, 2015, pp. 1-6: IEEE.

[101] A. Vangili and K. Thangadurai, "Detection of black hole attack in mobile ad-hoc networks using ant colony optimization–simulation analysis," *Indian Journal of Science and Technology*, vol. 8, no. 13, 2015.

[102] G. Singh, N. Kumar, and A. K. Verma, "Ant colony algorithms in MANETs: A review," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 1964-1972, 2012.

© COPYRIGHT UPM