A NEIGHBOR’S TRUST BASED MODEL FOR PREVENTION OF BLACK HOLE ATTACK IN WIRELESS MOBILE AD HOC NETWORKS

TANYA KOOHPAYEH ARAGHI

A prject submitted in partial fulfilment of

the requirements for the award of the degree of

Master of Computer Science (Information Security)

Advanced Informatics School

Universiti Teknologi Malaysia

JUNE 2013

I declare that this thesis entitled “*A Neighbour’s Trust Based Model for Prevention of Black Hole Attack in Wireless Mobile Ad Hoc Networks* “is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature: ....
Name: Tanya Koohpayeh Araghi
Date: JUNE 2013

Dedicated to

My beloved parents, my dearest siblings, and to all whom were beside me

ACKNOWLEDGEMENT

It is almost difficult for me to give enough thanks to all the people who have contributed to this study at Universiti Teknologi Malaysia as it was to write this thesis.

I am very fortunate to have had Dr. Mazdak Zamani as my supervisor. I am deeply indebted to him whose guidance, inspiration, and suggestions helped me finish this work. I would like to express my deepest appreciation to him. I appreciate Universiti Teknologi Malaysia, and Advanced Software Engineering Faculty of Computer Science and Information System. I am grateful to all my friends who made the times I spent in this university both rewarding and enjoyable.

I wish to express my gratitude to all those who have supported and helped me throughout my master, and enabled me to present this work. I am very grateful to my parents, for their love, understanding and support at every step. Without them, I would never be able to accomplish all the things that I have done throughout these years. Finally, I would like to thank my siblings, specially my brother, Sagheb Koohpayeh Araghi, who has always been encouraging and helpful through the difficult moments of my life and my dear friends Sima Boujarian and Elham Majd for accompanying me in every moment, and Abang Abdul Rasyid for translating the abstract in Malay.

ABSTRACT

Implementing Ad hoc networks are becoming very prevalent during recent years. Security is the most important issue for developing mobile ad hoc networks (MANETs). They expose to various kinds of attacks because of their unique nature in which every node can easily join to network or leave it. Black hole attack is the most probable attack in MANET. In this research we proposed a model for prevention of this attack. It judges on route replies coming from the intermediate node based on a trusted third party which is the destination node. If the source node received an acknowledgement on the route replies sending by an intermediate node, from destination during a specific time, it decides that the path is safe and intermediate node is not malicious. Meanwhile a counter will be set for counting the number of times that each intermediate node introduced a wrong route reply. Every node that proposes a wrong route reply will be recorded in a black list. The process also will be checked for all one hop neighbors of the suspicious node and the history of these nodes will be gathered in the black list, if they proposed a wrong route reply during the route discovery process. When the counter for each node exceed from a specific value, the suspicious nodes will be introduced as black holes and an alarm will be notified to all nodes in the network to remove these malicious nodes from their routing tables. Experimental results show that this model proposes a high rate of packet delivery ratio, with 88% improving network throughput compared with a network exposing in attack situation and decreasing the rate of end to end delay with 38% less than attack situation.

ABSTRAK

Perlaksanaan rangkaian Adhoc menjadi sangat meluas sejak beberapa tahun kebelakangan. Keselamatan merupakan isu penting begi membangunkan rangkaian adhoc mudah alih (MANETs). Mereka tededah kepada pelbagai jenis serangan kerana sifat mereka yang unik di mana setiap nod boleh menyertai atau keluar dari sesebuah rangkaian dengan mudah. . serangan black hole ada serangan yang berkemungkinan besar untuk terjadi. Dalam kajian ini, kami mencadangkan satu model untuk mencegah serangan ini. Ia membuat keputusan berdasarkan maklumbalas nod yang dating dari nod pertengahan berdasarkan kerpercayaan pihak ketiga iaitu destinasi nod, Apabila sumber nod menerima maklumbalas mengenai rangkaian melalui node pertengahan oleh nod destinasi dari semasa ke semasa, ia kemudiannya akan membuat keputusan yang ia adalah jalan yang selamat dan nod petengahan adalah tidak berniat jahat. Sementara itu, pengiraan akan dilakikan setiap kali nod menggunakan maklumbalas yang salah. Setiap nod yang mencadangkan laluan yang salah akan direkodkan di dalam senarai hitam. Proses ini juga akan diperiksa untuk semua destinasi terus yang bersebelahan yang mencurigakan dan rekod nod ini akan dikumpul di dalam senarai hitam. Jika mereka mencadangkan maklumbalas yang silap semasa proses penenemuan laluan. Apabila pengiraan mereka untuk setiap nod melebihi nilai tertentu, nod yang mencurigakan akan diperkenalkan sebagai lubang hitam dan penggera akan dimaklumkan kepada semua nod dalam rangkaian untuk membuang nod yang berniat jahat dari laluan mereka. Keputusan eksperimen menunjukkan bahawa model ini mencadangkan kadar yang tinggi nisbah penghantaran paket, dengan 88% meningkatkan keupayaan rangkaian berbanding dengan rangkaian yang terdedah dalam keadaan serangan dan mengurangkan kadar penangguhan hujung ke hujung sehingga 38%.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABM	-	Anti black hole mechanism
AODV	-	Ad hoc on demand distance vector
BSS	-	Basic service set
CA	-	Certificate authority
CL$_{IN}$	-	The concern level of intermediate node
CL$_{NHN}$	-	The concern level of next hop node
CRRT	-	Collect route reply table
DPRAODV	-	Detection, prevention and reactive AODV
DOS	-	Denial of service
DRI	-	Data routing information
DSDV	-	Destination sequenced distance vector
DSR	-	Dynamic source routing
DV	-	Distance vector
FRQ	-	further request
IDS	-	Intrusion detection system
IN	-	Intermediate node
KDC	-	Key distribution centre
MAC	-	Message authentication code
MANET	-	Mobile ad hoc networks
MODV	-	Modified ad hoc on demand distance vector
MRREP	-	More route reply
MRREQ	-	More route request
NHN	-	Next hop node
PCBHA	-	Prevention of cooperative black hole attack

PKI	-	Public key infrastructure
PRF	-	Pseudo random function
RERR	-	Route error
RREP	-	Route reply
RREQ	-	Route request
SN	-	Source node
T_{MRREP}	-	Time of receiving RREP
T_{TO}	-	T of time out
WLAN	-	Wireless local area networks
WPAN	-	Wireless personal area networks
WWAN	-	Wireless wide area networks
ZRP	-	Zone routing protocol

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Having an infrastructure less network was a desire that first developed in the 1970s. Since then, the knowledge of both computers and radio communication has outstanding growth led to the inception of wireless network (Chandra, 2011).

Instead of using physical cables, some kinds of radio frequencies in the air are utilized for data transmission in wireless networks. Wireless networks shaped by hosts and routers (Bala *et al.*, 2010).

They are categorized in wireless personal area networks (WPAN), local area networks (WLAN), and wide area networks (WWAN) based on their coverage area. Basic Service Set (BSS) is the essential building block of an 802.11 network, which is simply a group of stations that communicate with each other. While at least two stations communicate with each other, they considered as members of the basic service area (BSS). The 802.11 standard has two BSS modes. These are ad-hoc and infrastructure networks (Dokurer, 2006). Figure 1.1 illustrates these two types of networks.

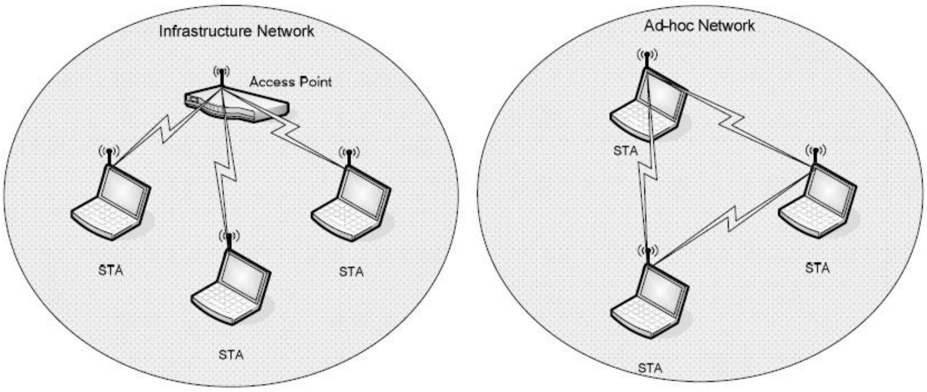

Figure 1.1: Infrastructure Network and Ad-hoc Network (Dokurer, 2006)

1.2 Mobile Ad hoc Networks (MANETs)

Ad hoc networks are a set of mobile nodes communicating with each other using multi-hop links. The networks that support ad hoc architectures are typically called mobile ad hoc networks (MANET) (Bala *et al.*, 2010).

A mobile ad-hoc network (MANET) includes wireless devices, generally called "nodes," that exchange data without having a central access point. Nodes are devices like, laptop, mobile phone, MP3 player, personal digital assistants (PDA) and personal computer taken part in the network and are mobile (Weerasinghe and Fu, 2007). Figure 1.2 shows heterogeneous devices constitute a MANET.

Such devices can communicate with the nodes within their radio range or outside their radio range via relay nodes. MANETs are adaptive and self organizing. Since they do not rely on any network entities, they can be formed on the fly without any extra infrastructure. There is an enormous heterogeneity between devices because any device equipped with wireless communication can connect to the ad-hoc network. Consequently, power consumption, storage, communication and computation and of these devices are various extremely (Chandra, 2011).

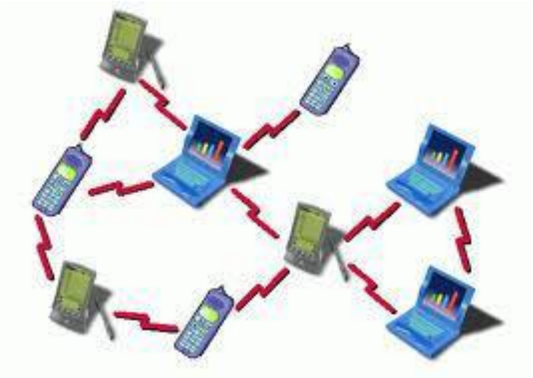

Figure 1.2: Heterogeneous mobile device ad hoc networks (Chandra, 2011)

Routing and management are also performed cooperatively by each node in the network. Hence their transmission power is limited multi hop architecture is needed for communication of nodes through the network. In this architecture, each node works either as a host or as a router that forwards packets for other nodes that may not be in a direct range of communication. Nodes participate in an ad hoc route discovery protocol which figures out multi hop routes through the network between any two nodes. They create routes among themselves dynamically to form their own wireless network on the fly (Weerasinghe and Fu, 2007).

The popularity of MANETs is increasing rapidly since they do not depend on any pre-infrastructure and can be formed spontaneously. They grant an enormously flexible communication method for every situation with geographical or territorial constraints in which network system without any fixed infrastructure is necessary (Weerasinghe and Fu, 2007).

Their application appears in managing natural disasters, battlefields, and historical places. Figure 1.3 shows the application of MANETs in a battle field (Wu *et al.*, 2002).

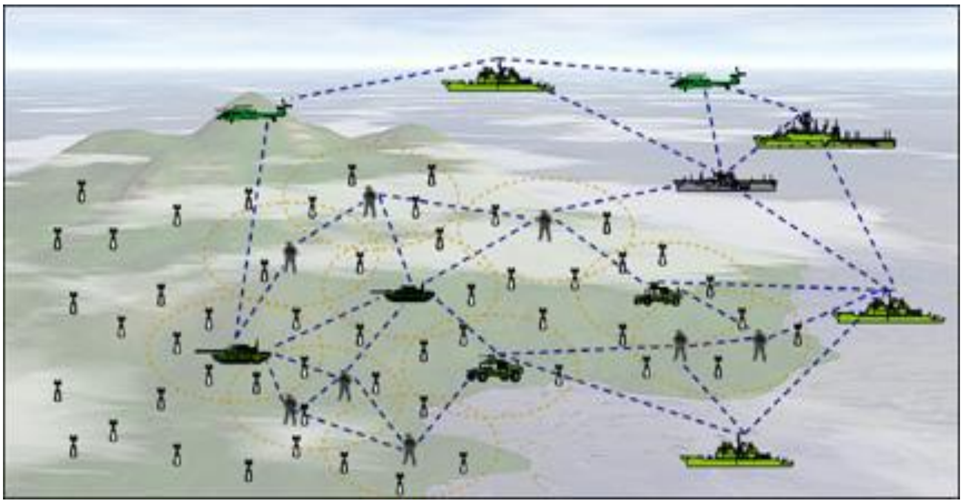

Figure 1.3: Battlefields (Chandra, 2011)

1.3 Background of the Problem

In mobile ad hoc networks, nodes also execute the task of routers that discover and maintain routes to other nodes. This fact can be regarded as a vital weakness since a compromised node could provide erroneous information in forwarding traffic or simply preventing it. Furthermore, routing protocols are very fragile in term of security.

Some causes of the problems related to the nature of MANET and its routing protocols are described as below.

1.3.1 Infrastructure of ad hoc networks

Lack of predetermined infrastructure in ad hoc networks, nodes compelled to deal with the routing of packets. Every node depends on the other neighboring nodes to route data packets (Deshpande, 2007).

1.3.2 Implicit trust relationship among neighbors

Ad-hoc routing protocols assume that all participants are honest. This hypothesis allows malicious nodes to try to paralyze the network thoroughly , by providing incorrect information which breaks the principles of Network Security (Tsou *et al.*, 2011). Hence the primary goal of routing protocols is to establish a safe and optimal route between participant nodes (Weerasinghe and Fu, 2007).

Any attack in routing phase may distort the overall communication and the network can be paralyzed thoroughly. Therefore in comparison to their wired counterparts the nodes in ad hoc networks are more vulnerable to security attacks (Anita and Vasudevan, 2010).

1.3.3 Problems in relation to wireless communication

Wireless channels have a weak protection to noise and signal interferences, so routing related in the control messages might be tempered. Broadcasting wireless channels permits malicious nodes to access to the network, eavesdrop and inject messages simply. A malicious intruder can spy on the channel and disrupt or alter the information within the network (Mohammed and Dargin, 2010).

1.3.4 Dynamic topology of ad-hoc networks

The mobility-aspect of ad-hoc network effects on the organization of nodes in MANETs because they included nodes that may change their locations frequently. Based on this fact, the dynamic topology of these kinds of networks, is a main characteristic that causes problems (Deshpande, 2007).

Mobile Nodes change their position, therefore the network topology change dynamically. This fact allows any malicious node to connect to the network devoid of detection (Tsou *et al.*, 2011). Unattended nodes can be easily stolen. An attacker may use a stolen node for developing a malicious decoy, and set it close to the original nodes. This can result to impersonation and information exposure (Mohammed and Dargin, 2010).

1.3.5 Restricted computing resources in MANET nodes

Attacks can be planned to force nodes to exceed their bandwidth, processing power, RAM storage, or battery life restrictions. Routing table overflow and energy consummation are examples of such attacks (Tsou *et al.*, 2011).

1.4 Problem Statement

The origin of the problem goes back to the route finding in routing protocols such as AODV and DSR in which not only the destination node can send a route reply message (RREP), but also an intermediate node who knows a valid route can send the RREP message to answer to the sender. An attacker that obtains a route request message (RREQ) can misuse of this problem by forwarding a RREP package to the sender, claiming that the destination node is a node which is only some hops away from the invader. Then the attacker will masquerade having the shortest path and be contained within the transmission route. All in all, the problem statement can be regarded as sending fake route replies (RREP) from a malicious intermediate node. This is possible either by pretending the shortest route or the highest sequence number (the highest sequence number represents the freshest route). The related attack trees shown in Figure.1.4 which illustrate the attack tree in detail in Figure.1.5 (represented by a triangle) included the kernel of the black hole attack (Ebinger and Bucher, 2006).

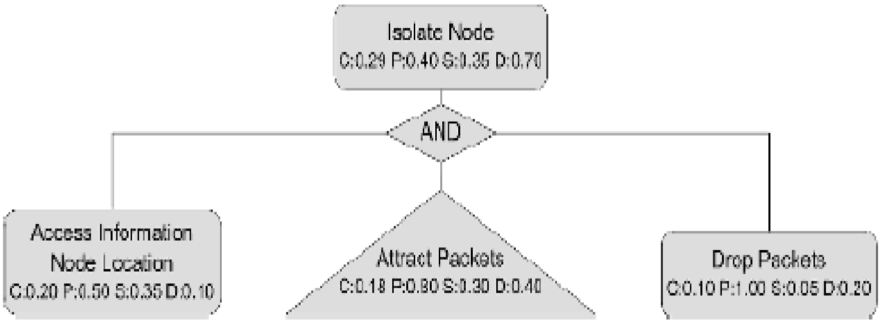
Isolate Node
C:0.29 P:0.40 S:0.35 D:0.70
AND
Access Information
Node Location
C:0.20 P:0.50 S:0.35 D:0.10
Attract Packets
C:0.18 P:0.80 S:0.30 D:0.40
Drop Packets
C:0.10 P:1.00 S:0.05 D:0.20

Figure.1.4: Black hole attack to isolate a node (Ebinger and Bucher, 2006)

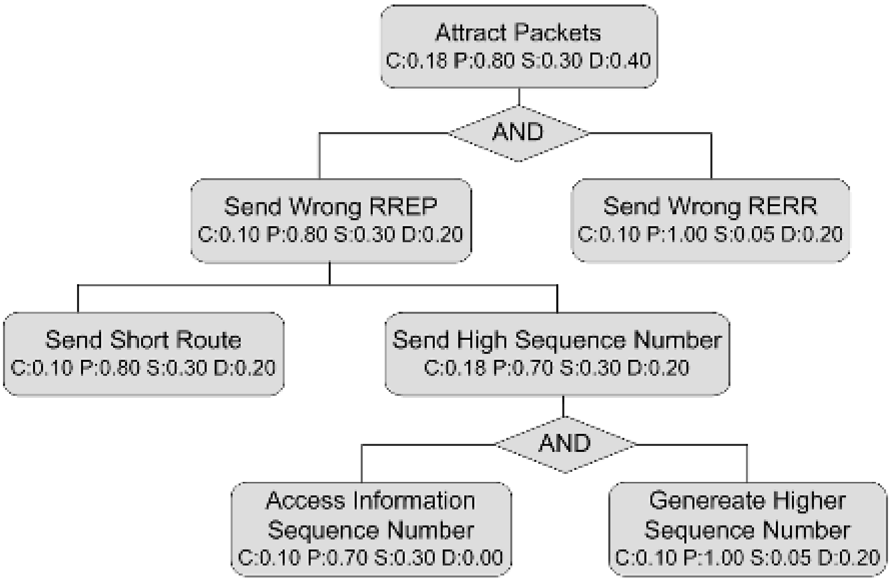
Attract Packets
C:0.18 P:0.80 S:0.30 D:0.40
AND
Send Wrong RREP
C:0.10 P:0.80 S:0.30 D:0.20
Send Wrong RERR
C:0.10 P:1.00 S:0.05 D:0.20
Send Short Route
C:0.10 P:0.80 S:0.30 D:0.20
Send High Sequence Number
C:0.18 P:0.70 S:0.30 D:0.20
AND
Access Information
Sequence Number
C:0.10 P:0.70 S:0.30 D:0.00
Genereate Higher
Sequence Number
C:0.10 P:1.00 S:0.05 D:0.20

Figure.1.5: Attack tree of a black hole attack (Ebinger and Bucher, 2006)

1.5 Project Objectives

The objectives of this study are as below:

- To explore existing models for preventing black hole attack in MANETs.
- To propose and develop a model to prevent black hole attack in MANETs.
- To evaluate the effectiveness of the proposed model against black hole attack.

1.6 Research Questions

The research questions of this study are as below:

- How do current methods detect and prevent Black hole attack in MANETs?
- How can we detect and prevent Black hole attack in MANETs?
- How can we measure the performance of the proposed model against Black hole attack?

1.7 Project Aim

The aim of the study is to provide a model for preventing the black hole attack in MANETs. Firstly, studying the current algorithms regarding to the advantages and disadvantages of them, and investigating the criteria in which black hole attack misused, establish a safe route and detect the malicious node in an ad hoc network who disorders transmission of data by feeding wrong routing information (Agrawal *et al.*, 2008); Then proposing a new model to overcome this kind of misbehavior routing.

1.8 Scope of the Study

The scope of this research is wireless mobile ad hoc network which focuses on the black hole attack in MANETs, related methods in prohibition and providing a secure model for preventing this kind of attack.

Since, in contrast to wired networks, each node in an ad-hoc network forwards packets to the other peer nodes, the wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is a blurry boundary separating the inside network from the outside world. Therefore routing protocols play an imperative role in the creation and maintenance of nodes connections. Although several secure routing protocols are proposed for security issues in MANET, the computation overhead involved in them is awful and often suffers from scalability problems. As a preventive measure, the packets can be signed carefully, but in black hole attack, the attacker can simply drop the packet passing through it. Therefore, secure routing cannot resist such internal attacks (Raj and Swadas, 2009). Hence, in this research, it is intended to use AODV, which is a very popular reactive routing protocol in MANETs. The software which is going to be used for this purpose would be the NS2 network simulator.

1.9 Significance of the Study

The black hole attack is one of the first active attacks in MANETs. It is very prevalent in ad hoc networks with the probability of 72% and damage of 60% (Ebinger and Parsons, 2009). Considering such problems, the necessity of study against black hole attack is observed essentially. By this research it is aimed to resolve some problems related to this attack and find a method for preventing it.

1.10 Summary

Mobile ad hoc networks are efficient because of easy and fast deployment. However they are very vulnerable compared with their wired peers. In this chapter, the most important challenges that MANETs faced described. Black hole attack is one of the most prevalent attacks in MANETs with a high rate of damage. Hence in this study, it is aimed to find a solution to defend against this attack.

REFERENCES

Agrawal, P., Ghosh, R. K., and Das, S. K. (2008). *Cooperative black and gray hole attacks in mobile ad hoc networks,* 310-314.

Agrawal, S., and Jaiswal, S. (2012). Study to Eliminate Threat of Black Hole of Network Worms in MANET.

Al-Shurman, M., Yoo, S. M., and Park, S. (2004). *Black hole attack in mobile ad hoc networks*, 96-97.

Anita, E. A. M., and Vasudevan, V. (2010). Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining. *International Journal of Computer Applications IJCA, 1*(12), 22-29.

Bala, A., Kumari, R., and Singh, J. (2010). Investigation of Blackhole Attack on AODV in MANET. *Journal of Emerging Technologies in Web Intelligence, 2*(2).

Chandra, B. (2011). *Counter attack as a defense mechanism in ad hoc mobile wireless networks.* Oklahoma State University.

Deshpande, V. S. (2007). Security in Ad-Hoc Routing Protocols.

Djahel, S., Naït-Abdesselam, F., and Zhang, Z. (2011). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. *IEEE Communications Surveys and Tutorials, 13*(4), 658-672.

Dokurer, S. (2006). *Simulation of Black hole attack in wireless Ad-hoc networks*: Atılım University.

Dokurer, S., Erten, Y. M., and Acar, C. E. (2007). *Performance analysis of ad-hoc networks under black hole attacks,* 148-153.

Ebinger, P., and Bucher, T. (2006). Modelling and analysis of attacks on the MANET routing in AODV (Vol. 4104 LNCS, pp. 294-307).

Ebinger, P., and Parsons, M. (2009). *Measuring the impact of attacks on the performance of mobile ad hoc networks,* 163-164.

Garg, V. (2011). Mitigating Multiple Black Hole Attack using DRI in Wireless Ad Hoc Networks. *IJCST, 2*(4, Oct . - Dec. 2011).

Gorantala, K. (2006). Routing protocols in mobile ad-hoc networks. *Master's Thesis in Computing Science, June, 15*.

Jathe, S. R., and Dakhane, D. M. (2012). A Review Paper on Black Hole Attack and Comparison of Different Back Hole Attack Techniques. *International Journal of Cryptography and Security, 2*(1), 22-26.

Klein-Berndt, L. (2001). A quick guide to AODV routing. *National Institute of Standards and Technology*.

Lin, C. (2004). AODV routing implementation for scalable wireless Ad-hoc network simulation (SWANS). *httpy/jist. ece. cornell. edu/docs/040421-swans-ao dv. pdf.*

Liu, C., and Kaiser, J. (2003). *A survey of mobile ad hoc network routing protocols*: Universität Ulm, Fakultät für Informatik.

Min, Z., and Jiliu, Z. (2009). *Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks,* 26-30.

Mohammed, E., and Dargin, L. (2010). *Routing Protocols Security in Ah Hoc Networks.* Dargin,Oakland University School of Computer Science and Engineering CSE 681 Information Security.

Nasser, N., and Chen, Y. (2007). *Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks.* Paper presented at the Communications, 2007. ICC'07. IEEE International Conference on, 1154-1159.

Panda, M. G. (2012). Prevention of Black hole Attack in AODV protocols for Mobile Ad Hoc Network by Key Authentication. *Prevention, 2*(3).

Patcha, A., and Mishra, A. (2003). *Collaborative security architecture for black hole attack prevention in mobile ad hoc networks.* Paper presented at the Radio and Wireless Conference, 2003. RAWCON'03. Proceedings, 75-78.

Raj, P. N., and Swadas, P. B. (2009). DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet. *arXiv preprint arXiv:0909.2371*.

Raja Mahmood, R., and Khan, A. (2007). *A survey on detecting black hole attack in AODV-based mobile ad hoc networks.* Paper presented at the High Capacity Optical Networks and Enabling Technologies, 2007. HONET 2007. International Symposium on, 1-6.

Ramaswamy, S., Fu, H. R., and Nygard, K. E. (2005). Simulation study of multiple black holes attack on mobile ad hoc networks. *ICWN '05: Proceedings of the 2005 International Conference on Wireless Networks*, 595-602.

Reddy, K., and Thilagam, P. (2012). Taxonomy of Network Layer Attacks in Wireless Mesh Network. *Advances in Computer Science, Engineering & Applications*, 927-935.

Shoja, M. K., Taheri, H., and Vakilinia, S. (2011). *Preventing black hole attack in AODV through use of hash chain*, 1-6.

Sklyarenko, G. (2006). Seminar Technische Informatik, Institut fur Informatik. *Freie Universitat Berlin*.

Song, J. H., Wong, V. W. S., and Leung, V. (2004). *A framework of secure location service for position-based ad hoc routing.* Paper presented at the Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks, 99-106.

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.

Su, M. Y. (2012). A Study of Deploying Intrusion Detection Systems in Mobile Ad Hoc Networks. *Lecture Notes in Engineering and Computer Science, 2198*.

Tamilselvan, L., and Sankaranarayanan, V. (2008). Prevention of co-operative black hole attack in MANET. *Journal of Networks, 3*(5), 13-20.

Tsou, P. C., Chang, J. M., Lin, Y. H., Chao, H. C., and Chen, J. L. (2011). *Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs*, 755-760.

Venkanna, U., and Velusamy, R. L. (2011). *Black hole attack and their counter measure based on trust management in MANET: A survey*, 232-236.

Weerasinghe, H., and Fu, H. (2007). Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. *International Journal of Software Engineering and Its Applications, 2*(3), 362-367.

Wu, B., Chen, J., Wu, J., and Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. *Wireless Network Security*, 103-135.

Wu, S. L., Tseng, Y. C., Lin, C. Y., and Sheu, J. P. (2002). A multi-channel MAC protocol with power control for multi-hop mobile ad hoc networks. *The Computer Journal, 45*(1), 101-110.

Yu, C. W., Wu, T. K., Cheng, R. H., and Chang, S. C. (2007). A distributed and cooperative black hole node detection and elimination mechanism for ad hoc networks (Vol. 4819 LNAI, pp. 538-549).

Yu, C. W., Wu, T. K., Cheng, R. H., Yu, K. M., and Chang, S. C. (2009). A distributed and cooperative algorithm for the detection and elimination of multiple black hole nodes in ad hoc networks. *IEICE Transactions on Communications, E92-B*(2), 483-490.

Zhang, X., Sekiya, Y., and Wakahara, Y. (2009). *Proposal of a method to detect black hole attack in MANET*, 149-154.