UNIVERSITI PUTRA MALAYSIA

SECURE AdHoc ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL USING MEDIA ACCESS CONTROL AND SYMMETRIC ENCRYPTION AGAINST BLACK HOLE AND DDoS ATTACKS IN MANET

SAMIA KHAN

FK 2018 112

SECURE AdHoc ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL USING MEDIA ACCESS CONTROL AND SYMMETRIC ENCRYPTION AGAINST BLACK HOLE AND DDoS ATTACKS IN MANET

By

SAMIA KHAN

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

June 2018

DEDICATIONS

In the name of Allah, Most Merciful, Most Gracious.
This thesis is dedicated to
My beloved parents for their substantial support, endless encouragement and for being a great source of motivation:
Mr. and Mrs. Khan

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

SECURE AdHoc ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL USING MEDIA ACCESS CONTROL AND SYMMETRIC ENCRYPTION AGAINST BLACK HOLE AND DDoS ATTACKS IN MANET

By

SAMIA KHAN

June 2018

Chairman : Fazirulhisyam Bin Hashim, PhD
Faculty : Engineering

The Mobile Ad hoc Network (MANET) is an infrastructureless network that has applications in many fields. MANETs can change locations and configure themselves on the fly; the nodes are self-configuring and able to self-organize. For data communication, nodes in the MANETs act as router to forward data packet to other nodes in the network. To communicate in the network, the nodes need routing protocol to establish a route and exchange the data in a secure way. Ad hoc On Demand Distance Vector (AODV) is one of the frequently used routing protocols due to its reactive nature advantage. Nevertheless, AODV has the disadvantage of being attacked by various types of attacks, specifically black hole attacks and Distributed Denial of Service (DDoS) attacks where it publicizes itself by announcing that it has the shortest path to the destination by altering the important routing parameters. These threats are difficult to handle because of their characteristics, like the huge scale of botnets and the dynamic nature of attacking, which constitutes a DDoS attack. DDoS attacks should be handled and mitigated directly from the network as early as possible. Many researchers have come up with a number of research work for defending against these attacks. However, most of these solutions lead to the increase in routing overhead which affects the overall performance of the network. The main challenge in MANETs is to come up with a secure routing protocol that is lightweight and whose implementation results in less overhead, better performance and a secure network. For that reason, a lightweight defense mechanism that can secure the network from the attackers is resourceful as the cooperation between the neighbouring nodes is counted in MANETs. This research focuses mainly on a defense against the Black Hole and DDoS attacks which involves two authentication levels: a) layer-2 authentication, and b) symmetric encryption on the control packets to secure the established path from AODV routing before exchanging the data. This is done by modifying the conventional AODV routing protocol. The primary focus of this approach is the sub layer that is layer 2 of the Open Systems Interconnections model (OSI), which uses the Media Access Control (MAC) authentication for checking the validation and authenticity of the nodes that want to participate in the network. Both routing information and the MAC information are specifically checked for securing the network. The solution is implemented in the AODV protocol and tested on various scenarios in order to achieve the optimum results. The trace file which is the output from the Network Simulator 2 (NS2) shows better improvement over existing approaches. The analysis shows good network performance with maximum average throughput of 96.5% and reduced routing overhead of 4.71%, offering true positive detection rate at maximum value of 92%. Moreover, this proposed solution endeavours higher packet delivery ratio with relatively less end to end delay (EED) when compared to two recent research works (LSAM and HMAC).

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

PROTOKOL PENGHALAAN VEKTOR JARAK ATAS PERMINTAAN AD HOC YANG SELAMAT MENGGUNAKAN KAWALAN AKSES MEDIA DAN PENYULITAN SIMETRIK TERHADAP LUBANG HITAM DAN SERANGAN PERKHIDMATAN PENAFIAN TERAGIH PADA RANGKAIAN AD HOC BERGERAK

Oleh

SAMIA KHAN

Jun 2018

Pengerusi : Fazirulhisyam Bin Hashim, PhD
Fakulti : Kejuruteraan

Rangkaian ad hoc mudah alih (MANET) adalah rangkaian kurang infrastruktur yang mempunyai aplikasi dalam banyak bidang. MANET boleh mengubah lokasi dan mengkonfigurasi dirinya dengan cepat, nod-nod itu dapat mengkonfigurasi sendiri dan dapat mengaturkendiri. Untuk komunikasi data, nod dalam MANET bertindak sebagai penghantar untuk meneruskan paket data ke nod lain dalam rangkaian. Untuk berkomunikasi dalam rangkaian, nod memerlukan protokol penghalaan untuk menubuhkan laluan dan saling menukar data dengan cara yang selamat. Vektor Jarak atas Permintaan segera “ad hoc” (AODV) adalah salah satu protokol penghalaan yang sering digunakan kerana kelebihan reaktif semulajadinya. Walau bagaimanapun, AODV mempunyai kelemahan boleh diserang oleh pelbagai jenis serangan khususnya serangan lubang hitam dan serangan Penyebaran Penafian Perkhidmatan (DDoS) yang dimana ia mempublikasikan dirinya dengan mengumumkan bahawa ia mempunyai jalan terpendek ke destinasi dengan mengubah parameter-parameter laluan yang penting. Ancaman ini sukar untuk ditangani kerana ciri-ciri mereka seperti botnets berskala besar dan serangan yang bersifat dinamik. Inilah yang membentuk Serangan Penyebaran Penafian Perkhidmatan (DDoS). Serangan DDoS harus ditangani dan dikurangkan secara langsung dari rangkaian seawal mungkin. Ramai penyelidik tampil dengan banyak penyelidikan untuk mempertahankan serangan ini; namun kebanyakan daripada penyelesaian ini membawa kepada peningkatan penghalaan langkauan atas (overhead) yang mempengaruhi prestasi rangkaian. Cabaran utama dalam MANET adalah untuk menghasilkan protocol penghalaan laluan selamat yang ringan dan pelaksanaannya menghasilkan kurang langkauan atas (overhead), prestasi yang lebih baik dan rangkaian yang selamat. Atas sebab itu, mekanisma pertahanan yang ringan yang dapat menjamin jaringan dari serangan adalah terlalu banyak kerana kerjasama antara nod-nod berhampiran dihitung dalam MANET. Penyelidikan ini memberi tumpuan kepada pertahanan dan pengesanan terhadap serangan Black Hole dan DDoS yang melibatkan secara asasnya dua tahap pengesahan; a) pengesahan lapisan-2, dan b) enkripsi simetrik untuk paket kawalan untuk memastikan laluan yang ditubuhkan sebelum pertukaran data. Ini dilakukan dengan mengubah suai protokol penghalaan AODV asli. Tumpuan utama dalam pendekatan ini ialah sub-lapisan yang merupakan lapisan 2 sistem OSI yang menggunakan pengesahan Kawalan Akses Media (MAC) untuk memeriksa pengesahan dan ketulenan nod yang ingin menyertai rangkaian. Kedua-dua maklumat laluan dan maklumat MAC diperiksa khas untuk memastikan keselamatan rangkaian. Penyelesaian ini dilaksanakan dalam protokol AODV dan diuji pada pelbagai senario untuk mencapai hasil yang optimum. Fail jejak yang merupakan hasil dari simulator rangkaian 2 (NS2) menunjukkan penambahbaikan berbanding pendekatan yang sedia ada. Analisis ini menunjukkan prestasi rangkaian yang baik dengan daya pemprosesan purata maksimum 96.5% dan langkauan atas penghalaan dikurangkan 4.71%, memberikan kadar pengesanan positif maksimum 92%. Tambahan lagi, penyelesaian yang dicadangkan ini mengupayakan nisbah penghantaran packet yang tinggi dengan mengurangkan kelewatan hujung ke hujung (EED) apabila dibandingkan dengan dua kerja penyelidikan terkini (LSAM dan HMAC)

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my supervisor, Dr. Fazirulhisyam Hashim, for his generous support and great encouragement to conduct this research as well as his valuable comments to enhance the quality of the dissertation.

Furthermore, I am very grateful to the members of my supervisory committee, Prof. Dr. Fadlee bin A Rasid and Prof Dr. Thinagaran Perumal, for their help and support for the completion of this thesis. Lastly, I would like to appreciate the department staff and my research group fellows for their assistance during my research and thesis writing.

I certify that a Thesis Examination Committee has met on 8 June 2018 to conduct the final examination of Samia Khan on her thesis entitled "Secure AdHoc on Demand Distance Vector Routing Protocol Using Media Access Control and Symmetric Encryption Against Black Hole and DDoS Attacks in Manet" 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:

Muhammad Hafiz bin Abu Bakar, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Nurul Adilah Abdul Latiff, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Khaizuran Abdullah, PhD
Associate Professor
International Islamic University Malaysia
Malaysia
(External Examiner)

RUSLI HAJI ABDULLAH, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 27 September 2018

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 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: Samia Khan, GS44962

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: Dr. Fazirulhisyam b. Hashim

Signature: ________________________________

Name of Member of Supervisory Committee: Associate Professor Dr. Mohd Fadlee A. Rasid

Signature: ________________________________

Name of Member of Supervisory Committee: Dr.Thinagaran Perumal

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

AODV	Ad hoc On-Demand Distance Vector
ARQ	Automatic Repeat Request
AUC	Area under the curve
BH	Black hole
CBR	Constant Bit Rate
CAODV	Classified Ad hoc on Demand Vector
DoS	Denial of Service
DDoS	Distributed Denial of Service
DSDV	Destination-Sequenced Distance Vector
DSR	Dynamic Source Routing Protocol
EED	End-to-end Delay
FN	False Negative
FPR	False Positive Rate
FPS	Frame per second
GPS	Global Positioning System
HMAC	Hashed Message Authentication Code
IDEA	International Data Encryption algorithm
LSAM	Localised Secure Architecture for MANETs
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
NS	Network Simulator
OSI	Open Systems Interconnection
OLSR	Optimized Link State Routing Protocol
PDR	Packet Delivery Ratio
Pp	Propagation Period
PD	Processing Delay
PDR	Packet Delivery Ratio
Qu	Queuing Period
RREP	Route Reply
RREQ	Route Request
RERR	Route Error

ROC	Receiver Operating Characteristic
SAODV	Secured Ad hoc on demand Vector
SMN	Security Monitoring Nodes
TN	True Negative
TPR	True Positive Rate
Tr	Transmission Range
Tp	Transmission Period
TTL	Time to Live
ZRP	Zone Routing Protocol

CHAPTER 1

INTRODUCTION

1.1 Overview

Mobile Ad hoc network (MANET) is a blend of mobile nodes which defines that the nature of their network topology is dynamic. It fundamentally defines a modern framework that is shaped by a collection of remote versatile nodes, which exchange information using wireless medium. The nodes in MANET act as routers within the network for data transmission. Because of the novel characteristics of MANET like mobile and less expensive, MANET's are suitable for a wide range of uses like home appliances, critical applications, identifying events, mainly realted to sensor applications such as military surveillance, medical monitoring [1-6].

Routing is one of the main interests in MANET, as it is vulnerable to security errors because of the changing topology and flexibility of nodes. In the previous literature, the researchers have anticipated all nodes to be reliable[7, 8]. Although this scheme has been questioned as of late, many security threats have been developed to weaken MANET security [9] . These threats like black hole, grey hole, flooding threats. Compared to selfish and grey hole attacks, the blackhole and flooding threats severely affect the performance of the network.

A black hole attack is a type of Distributed Denial of Service (DDoS) attack where a router rejects packets instead of transmitting them. Usually, a DDoS tool is used to distribute this denial of service attack. The packets are recurrently lost, and it results in the loss of a network. The malicious router is always able to achieve the attacks selectively, which results in the detection of the attack extremely difficult.

The routing protocols are very prone to such attacks. And Black hole attack exploits this vulnerability and utilizes a malicious code to deceive the network. This node deceives the router by promoting itself to be considered as the shortest path to the nodes that it wants to disrupt. This attack aims at exploiting the routing protocol for the traffic to flow through a specific node that is under the control of the attacker. At the time of the Route Discovery Process, the source node transmits the RREQ packets to its transitional nodes so that it can find a new and unused path to reach the intended destination.

The source nodes are configured in such ways that the nodes that are harmful responds immediately to them. The source node ignores all the RREP messages from the other nodes regardless of their importance and considers the route discovery process to be completed. This is achieved by the harmful nodes by assigning a larger sequence number to the reply packet. Then the tracker lets go of the received messages instead of transmitting them according to the protocol.

In general, any MANET topology uses a transmission protocol to function, for example, Ad hoc On-Demand Distance Vector (AODV) and Destination-Sequenced Distance Vector (DSDV) and Dynamic Source Routing (DSR). Every single one of these protocols has its own strengths and weaknesses [10]. But compared to others, AODV offers decent delay and packet loss is small too [11]. In this way, it stands out amongst the most well-known routing protocols inside MANET. AODV is efficient in terms of power as it neither depends on activated connections nor reserves any data related to routing. Besides, nodes do not need to find or safeguard a way to another node unless the two nodes require information exchange [12].

At whatever point a node needs to send information to a destination, a route request packet is broadcasted to initiate the path discovery process to all the nodes in its neighbourhood. The intermediate node responds back with a route response packet (RREP) anytime it finds the recent route to the destination. A route error message packet will be sent to the source node in case of any link breakage to inform about the connection failure. Regardless of the good qualities of AODV [7], it is weak against the Black hole attack and DDoS attacks, since it doesn't have a strong characteristic for defending against security attacks [8]. For determining the fresh raw from source to destination, AODV makes use of two fields that are hop count and sequence number for information exchange. The best route to the destination comes with a high sequence number. The black hole node takes an advantage of this attribute by sending a fake response message by a forged announcement of having the highest sequence as well as less hop count.

Primarily, the black hole attack has two stages. The first stage is when it compromises the AODV by advertising itself as having the low hop count as well as high sequence number and displays itself as having a fresher route than any other node. The second stage is absorbing all the data packets by not allowing the packets to be forwarded that it gets from the source node [12]. In the long run, the entire system fails.

1.2 Problem Statement

In MANET, the black hole attacks have been a serious concern for a couple of years [10]. To exchange the information, MANET uses specific routing protocols from either of the two, reactive or proactive protocols. These black hole nodes usually misuse the AODV to execute malignant tasks. As AODV does not have a strong defense system to combat black hole attacks. So, the researchers have proposed distinctive sorts of ways to deal with this issue.

In MANETs one of the key concerns is performance to build up a transmission protocol. To enhance the quality of transmission in a MANETs network, routing protocol needs the best performance metrics like throughput, end to end delay, routing overhead and packet delivery ratio. During the process of communication, the routing protocol must have less routing overhead, minimal delay, maximum throughput delivery rate. The dynamic nature of topology and the security attacks can be a fewer reason for network deterioration.

From a security point of view, MANET has a distinctive identity and attributes that without a doubt bring out their own security concerns. Since MANET has an open network system, there is no managerial node to control the system and high flexibility. Numerous attacks can be performed in every correspondence layer. Each node can join the system effectively and it makes MANET weaker against an attacker's malignant activities. Compared to wired systems, MANET is more inclined to physical threats and it builds an ambiance for a few threats, like data modification attacks, eavesdropping attack, IP Spoofing attacks, DDoS attack. Adversary grabs the advantage of the weak design and uncertain implementation of routing protocols to alter the behaviour. These security attacks are not executed straightforwardly but rather they are provoked through the misconduct of the routing design. For example, Botnets, Man-in-the-Middle (MITM), DoS, DDoS attacks are activated and utilized by MANET specialized attacks like wormhole or black hole attacks [13, 14].

Under these limitations, the main challenge in MANET is how to build up a strong secure routing protocol that will wipe out the security threats existing in MANET without exhausting the complete performance. This thesis proposes an answer for routing protocol to cap the security concerns and provide better performance in MANET.

In MANET, the security method for routing protocols is separated in two classes in view of the security strategy, i.e. cryptographic system and trust-based component. In the first place, during the process of communication, the cryptographic method will protect the routing process in the network, routing maintenance and information exchange packets. Several traditional algorithms have been implemented to secure the data packets. Routing protocols using cryptographic methods has better performance measure execution compared to other methods like trust based mechanism or IDS mechanisms. A cryptography system is picked to enhance the security part of protocol because likely a secure AODV routing protocol is modified with a decent overall performance.

Different specialists utilized Intrusion detection systems (IDS) as a goal to disengage the black hole attacks in AODV [15]. This approach works by actualizing a standardized technique for the MANET to function. This methodology will incorporate all the legitimate tasks that could be possible in the regular situations and separate any task that falls outside the technique. This approach offers a tolerable delay, but it experiences a high false positive detection rate.

The proposed approach includes consolidating two basic approaches. The primary approach depends on the symmetric key encryption technique offering a prudent accuracy for detection as well as the slightest delay and overhead. The main hypothesis n is that by using the MAC authentication, the defense mechanism can be additionally enhanced if another phase is included as a tier of authentication. The basic goal of this research is to achieve minimal routing overhead, higher throughput, packet delivery ratio with an enhanced detection rate of malignant nodes using lightweight symmetric cryptographic algorithm.

1.3 Research Aim and Objectives

The quick advancement and wide utilization of MANET makes security as the most risky issue. As of late, the IDS framework is considered as a key that can be utilized to explain security challenges. Hence, the goal of this research is to propose a lightweight algorithm that can be utilized in MANETs. This research work presents a lightweight mechanism framework using MAC and encryption technique to secure MANETs from Black hole and DDoS attacks. In order to accomplish this aim, achieving the following objectives is the fundamental part of this thesis:

1. To design an efficient lightweight defense algorithm by modifying the AODV routing protocol for securing the route for data transmission in the MANETs.
2. To reduce the routing overhead that is increased by most of the securing mechanisms.
3. To improve the performance and defense of black hole nodes and DDoS in the network with the proposed modified AODV protocol using the Network Simulator 2 under different network parameters.

1.4 Thesis Scope

The extent of this work concentrates exclusively on the Distributed Denial of Service (DDoS) and black hole nodes that can be propelled against the AODV protocol by attackers. The black hole attack and DDoS attacks are hard to distinguish since the intruder imitates an existing node inside the MANET to carry out any noxious activity. In this research all the nodes are mobile in the topology. This work also analyses the Receiver Operating Characteristic analysis (ROC) that gives a detection rate of malicious nodes. Moreover, this work attempts to offer an analysis of ideal design where negligible delay is being obtained and a better PDR. The proposed approach will speculate the following assumptions:

1. The nodes in the network are reliable.
2. All node IDs are unique.
3. The black hole nodes and DDoS are external and passive attacks.

4. The black hole nodes are in a vital position that enables them to contribute in most system traffics.
5. The algorithm proposed is implemented before the route discovery phase.
6. The pioneer nodes do not take an interest in the information transmission.

As a proof of theory, the results obtained in this research after the implementation of proposed algorithm are contrasted and compared with two recent mechanisms, namely, LSAM [83] and HMAC [84].

1.5 Motivation

MANET is a system made out of an expansive number of nodes. These can be utilized to recognize any number of properties of a region. Cases incorporate temperature, weight, poisons, contaminations, and so on. Versatile impromptu sensor systems could be the way to future country security. The ongoing advances in MANET incorporates its subclass VANET (Vehicular Ad hoc Network).

The most recent case of MANETs is simply the Nissan's affirmation coordinated driving cars that will be self-governing 2020. This advancement in innovation is a capacity of V2V (vehicle to vehicle correspondence) and an example of MANETs. This has numerous points of interest: cars moving toward a visually impaired crossing point could caution each other of their reality. Cars going in escort could interlock their voyage control frameworks to give better movement stream.

A car in panic a could caution cars behind and help evade, or lessen the seriousness of, an accident. A car making a sudden, forceful redress could caution different cars of a potential circumstance.

Much like your cell phone consults with known WiFi center points to naturally interface when in go, cars could be driving around conveying solicitations to associate with different cars in range and subsequently make their own 'specially appointed' system, where cars would travel every which way as they came into and left range.

The security of MANET is a standout amongst the most other challenges. This fundamentally results because of the common characteristics of MANET, for example limited power, limited resources, no central authority, mobility of nodes and of course the absence of a strong defense mechanism.

To guarantee a safe transmission over MANET, a complete outline of various threats and their results is required. Some of the attacks like Wormhole attack, Denial of Service, Black hole attack, Sybil attack, flooding attack, impersonating and selfish node behaviour attack can target MANETs. A comprehensive summary of various security attacks on MANETs is reviewed in [16].

Mostly, MANET is more helpless to these sorts of threats since one node in the MANET will believe that every one of the neighbouring nodes is reliable [7]. MANET does not experience just the same sorts of threats like DoS, Spoofing of IP address or message falsification. Nonetheless, it additionally experiences new threats like the black hole attack, DDoS, worm hole attack that originate due to some characteristics of MANET. For example, the black hole attack appears when a node in the network advertises itself as a node having the fresh and the fastest route to the destination. This gives the malignant node the ability to embed itself in the middle of the transmitting nodes in the network. Subsequently, the noxious node absorbs all the packets it receives. MANET is weak when it comes to such attacks as the transmission is based on the authentic path from source to destination. Also, they lack the centralized authority for observing the malicious activity of any node.

The result of the research work on protecting the MANETs against the DDoS attacks and the black hole attack are the techniques that either require continuous monitoring of the nodes or requires performing some computational operations to the respective nodes in MANET which eventually exhausts the limited resources, like processing power, bandwidth and the memory of the nodes. Henceforth the main aim of this research is to defend and detect the black hole and DDoS attacks by introducing a modified AODV that can prevent the MANET from the black hole and DDoS by safeguarding the route from source to destination with less routing overhead and a better throughput and PDR.

1.6 Thesis Organization

This thesis indicates how black hole and DDoS attacks in MANET can be defended and distinguished effectively. The thesis is organized as follows. Chapter 1 covers the introduction and precise overview of the black hole and DDoS attacks in MANETs. Chapter 1 also highlights the problem statement, research objectives and scope of the research.

Chapter 2 presents the detailed description of the conventional security mechanisms used in MANETs. The main target of chapter 2 is the literature review on defending and detection of black hole and DDoS attacks. Next, this chapter portray in detail the structure of MANETs. After that, this section presents routing tables in MANET and their arrangements. Next, the security threats in MANET and its weaknesses are depicted. Then description of the black hole and DDoS attacks in detail is given and how they are destructive against AODV protocol. At last, in Chapter 2, related works is discussed and explanation of how our research work is better and distinct compared to others. Furthermore, it explains the significance of symmetric cryptographic solution.

Chapter 3 explains our proposed methodology for defending black hole and DDoS attacks in the network. Here, the layering approach is implemented, for monitoring the media access control (MAC) layer of the layer-2 and for higher security, the concept used is encryption and decryption of Route request packet (RREQ) using symmetric key exchange mechanism by modifying the AODV protocol and analyse it. Later the proposed method is implement in the AODV protocol in a way to obtain an improved performance and a better detection rate of malicious nodes.

Chapter 4 incorporates the results and discussion with the appropriate charts. Lastly, Chapter 5 is the conclusion of this dissertation highlighting the contributions followed by the future work.

BIBLIOGRAPHY

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–105, 2002.

[2] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Comput. Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[3] A. Boukerche, “Performance evaluation of routing protocols for ad hoc wireless networks,” *Mob. Networks Appl.*, vol. 9, no. 4, pp. 333–342, 2004.

[4] T. Sohraby, K., Minoli, D., Znati, *Wireless sensor networks: technology, protocols, and applications*, *John Wiley and Sons Ltd*, vol. 53, no. 9. 2013.

[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: an introduction,” *Ad hoc Netw.*, vol. 40, pp. 20–22, 2001.

[7] J. H. Cho, A. Swami, and I. R. Chen, “A Survey on Trust Management for Mobile Ad Hoc Networks,” *IEEE Commun. Surv. 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,” *Proc. IEEE*, vol. 98, no. 10, pp. 1755–1772, 2010.

[9] H. Nguyen and U. 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,” *Comput. Networks Distrib. Syst.*, 2003.

[11] N. S. M. Usop, A. Abdullah, A. F. A. Abidin, and others, “Performance evaluation of AODV, DSDV & DSR routing protocol in grid environment,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, 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,” *Network*, vol. 4, no. 3, pp. 498–500, 2013.

[13] A. Gagandeep and P. Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review,” *Int. J. Eng. Adv. Technol.*, no. 15, pp. 2249–8958, 2012.

[14] X. Yu, “A defense system on ddos attacks in mobile ad hoc networks,” 2007.

[15] R. Puttini, J.-M. Percher, L. Me, and R. De Sousa, “A fully distributed IDS for MANET,” *Proceedings. ISCC 2004. Ninth Int. Symp. Comput. Commun. (IEEE Cat. No.04TH8769)*, vol. 1, pp. 331–338, 2004.

[16] A. K. Rai, R. R. Tewari, and S. K. Upadhyay, “Different types of attacks on integrated manet-internet communication,” *Int. J. Comput. Sci. Secur.*, vol. 4, no. 3, pp. 265–274, 2010.

[17] 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.

[18] W. A. Xiong and Y. H. Gong, “Secure and highly efficient three level key management scheme for MANET,” *WSEAS Trans. Comput.*, vol. 10, no. 1, pp. 6–15, 2011.

[19] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[20] Z. Ye, S. V Krishnamurthy, and S. K. Tripathi, “A framework for reliable routing in mobile ad hoc networks,” in *Proceedings - IEEE INFOCOM*, 2003, vol. 1, pp. 270–280.

[21] S.-J. Lee and M. Gerla, “AODV-BR: backup routing in ad hoc networks,” *2000 IEEE Wirel. Commun. Netw. Conf. Conf. Rec. (Cat. No.00TH8540)*, vol. 3, pp. 1311–1316, 2000.

[22] A. Valera, W. K. G. Seah, and S. V. Rao, “Cooperative packet caching and shortest multipath routing in mobile ad hoc networks,” in *Proceedings - IEEE INFOCOM*, 2003, vol. 1.

[23] S. M. C. Vigila and K. Muneeswaran, “Implementation of text based cryptosystem using elliptic curve cryptography,” in *2009 1st International Conference on Advanced Computing, ICAC 2009*, 2009, pp. 82–85.

[24] D. Wadbude and V. Richariya, “An efficient secure AODV routing protocol in MANET,” *Int. J. Eng. Innov. Technol. Vol.*, vol. 1, pp. 274–279, 2012.

[25] P. Kuppuswamy, P. M. Appa, and D. S. Q. Y. Al-Khalidi, “A New Efficient Digital Signature Scheme Algorithm based on Block cipher,” *IOSR J. Comput. Eng.*, vol. 7, no. 1, pp. 47–52, 2012.

[26] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks,” *IEEE Wirel. Commun.*, vol. 14, no. 5, 2007.

[27] F. H. P. Fitzek and M. D. Katz, “Cooperation in nature and wireless communications,” in *Cooperation in Wireless Networks: Principles and Applications*, Springer, 2006, pp. 1–27.

[28] A. A. A. Alkhatib, G. S. Baicher, and W. K. Darwish, “Wireless sensor network-An advanced survey,” *Int. J. Eng. Innov. Technol.*, vol. 2, no. 7, pp. 355–369, 2013.

[29] A. Baadache and A. Belmehdi, “Avoiding Black Hole and Cooperative Black Hole Attacks in Wireless Ad hoc Networks,” *J. Comput. Sci.*, vol. 7, no. 1, p. 7, 2010.

[30] J. G. Ponsam and R. Srinivasan, “A Survey on MANET Security Challenges,, Attacks and its Countermeasures,” *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 1, pp. 274–279, 2014.

[31] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, “A survey on wireless multimedia sensor networks,” *Comput. Networks*, vol. 51, no. 4, pp. 921–960, 2007.

[32] P. R. Pereira, A. Grilo, F. Rocha, M. S. Nunes, A. Casaca, C. Chaudet, P. Almström, and M. Johansson, “End-To-End Reliability in Wireless Sensor Networks: Survey and Research Challenges,” *EuroFGI Work. IP QoS Traffic Control*, vol. 54, pp. 67–74, 2007.

[33] A. Bachir, M. Dohler, T. Watteyne, I. Member, and I. S. Member, “MAC Essentials for Wireless Sensor Networks MAC Essentials for Wireless Sensor Networks,” *Commun. Surv. {&} Tutorials*, vol. 12, no. 2, pp. 222–248, 2010.

[34] G. Meghan and G. M. Simon, “A comparative study of medium access control protocols for wireless sensor networks,” *Int. J. Commun. Netw. Syst. Sci.*, vol. 2, no. 08, p. 695, 2009.

[35] H. Frey, S. Rührup, and I. Stojmenović, “Routing in Wireless Sensor Networks,” in *Guide to Wireless Sensor Networks*, 2009, pp. 81–111.

[36] E. M. Royer and C. E. Perkins, “An implementation study of the AODV routing protocol,” *IEEE Wirel. Commun. Netw. Conf.*, vol. 3, pp. 1003–1008, 2000.

[37] 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.

[38] S. R. Biradar, H. H. D. Sarma, K. Sharma, S. K. Sarkar, and C. Puttamadappa, “Performance comparison of reactive routing protocols of MANETs using group mobility model,” in *2009 International Conference on Signal Processing Systems, ICSPS 2009*, 2009, pp. 192–195.

[39] 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.

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

[41] M. G. Zapata and N. Asokan, “Securing Ad Hoc Routing Protocols,” in *Proceedings of the 1st ACM workshop on Wireless security*, 2002, pp. 1–10.

[42] P. K. Maurya, G. Sharma, V. Sahu, A. Roberts, M. Srivastava, M. Scholar, and others, “An overview of AODV routing protocol,” *Int. J. Mod. Eng. Res.*, vol. 2, no. 3, pp. 728–732, 2012.

[43] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” 2003.

[44] L. Klein-Berndt, “A quick guide to AODV routing,” *Wirel. Commun. Technol. Group, NIST (http//w3. antd. nist. gov/wctg/aodv_kernel/)*, 2001.

[45] 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.

[46] T. Clausen and P. Jacquet, “Optimized link state routing protocol (OLSR) Report No.: 2070-1721,” 2003.

[47] S. Mohseni, R. Hassan, A. Patel, and R. Razali, “Comparative review study of reactive and proactive routing protocols in MANETs,” in *Digital ecosystems and technologies (DEST), 2010 4th IEEE international conference on*, 2010, pp. 304–309.

[48] 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.

[49] Z. J. Haas, M. R. Pearlman, and P. Samar, “The Zone Routing Protocol (ZRP) for Ad Hoc Networks,” *draftietfmanetzonezrp02 txt*. 2002.

[50] J. Schaumann, “Analysis of the zone routing protocol,” 2002.

[51] S. Sesay, Z. Yang, and J. He, “A survey on mobile ad hoc wireless network,” *Inf. Technol. J.*, vol. 3, no. 2, pp. 168–175, 2004.

[52] K. Biswas, M. Ali, and others, “Security threats in mobile ad hoc network.” 2007.

[53] 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.

[54] M. R. Ahmed, X. Huang, and D. Sharma, “A Taxonomy of Internal Attacks in Wireless Sensor Network,” *WorldAcademy ofScience, Eng. Technol.*, 2012.

[55] P. Vinayakray-Jani, “Security within ad hoc networks,” in *First PAMPAS Workshop*, 2002, pp. 66–67.

[56] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, “Security in mobile ad hoc networks: challenges and solutions,” *Wirel. Commun. IEEE*, 2004.

[57] R. H. Jhaveri, S. J. Patel, and D. C. Jinwala, “DoS Attacks in Mobile Ad Hoc Networks: A Survey,” in *2012 Second International Conference on Advanced Computing & Communication Technologies*, 2012.

[58] 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.

[59] D. B. Roy, R. Chaki, and N. Chaki, “A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks,” *arXiv Prepr. arXiv1004.0587*, 2010.

[60] N. Shanthi, L. Ganesan, and K. Ramar, “Study of different attacks on multicast mobile ad hoc network.,” *J. Theor. Appl. Inf. Technol.*, vol. 6, 2009.

[61] A. Vani and D. S. Rao, “Providing of secure routing against attacks in manets,” *Int. J. Comput. Appl. Vol.*, 2011.

[62] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish,” in *Procedia Computer Science*, 2016.

[63] H. Al Amri, M. Abolhasan, and T. Wysocki, “Scalability of MANET routing protocols for heterogeneous and homogenous networks,” *Comput. Electr. Eng.*, 2010.

[64] D. G. Padmavathi and M. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” *Int. J. Comput. Sci. Inf. Secur.*, 2009.

[65] 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.

[66] M. Al-Shurman, S.-M. Yoo, and S. Park, “Black hole attack in mobile ad hoc networks,” in *Proceedings of the 42nd annual Southeast regional conference*, 2004, pp. 96–97.

[67] 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,” *Int. J. Netw. Secur.*, 2007.

[68] H. Deng, W. Li, and D. P. Agrawal, “Routing security in wireless ad hoc networks,” *IEEE Commun. Mag.*, 2002.

[69] S. A. Arunmozhi and Y. Venkataramani, “DDoS Attack and Defense Scheme in Wireless Ad hoc Networks,” *arXiv Prepr. arXiv1106.1287*, 2011.

[70] M. Chhabra, B. Gupta, and A. Almomani, “A Novel Solution to Handle DDOS Attack in MANET,” *J. Inf. Secur.*, 2013.

[71] S. Saraeian, F. Adibniya, M. GhasemZadeh, and S. Abtahi, “Performance Evaluation of AODV Protocol under DDoS Attacks in MANET,” *Proc. World Acad. Sci. Eng. Technol. vol*, vol. 33, pp. 501–503, 2008.

[72] P. Yi, Z. Dai, S. Zhang, Y. Zhong, and others, “A new routing attack in mobile ad hoc networks,” *Int. J. Inf. Technol.*, vol. 11, no. 2, pp. 83–94, 2005.

[73] M. G. Zapata, “Secure ad hoc on-demand distance vector routing,” *ACM SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 6, no. 3, pp. 106–107, 2002.

[74] A. A. Pirzada and C. McDonald, “Secure routing with the AODV protocol,” in *Communications, 2005 Asia-Pacific Conference on*, 2005, pp. 57–61.

[75] M. Akhlaq, M. N. Jafri, M. A. Khan, B. Aslam, and others, “Addressing security concerns of data exchange in aodv protocol,” *World Acad. Sci. Eng. Technol.*, vol. 16, pp. 29–33, 2006.

[76] S. Eichler and C. Roman, “Challenges of secure routing in MANETs: A simulative approach using AODV-SEC,” in *2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS*, 2006.

[77] A. Dhaka, A. Nandal, and R. S. Dhaka, “Gray and black hole attack identification using control packets in MANETs,” *Procedia Comput. Sci.*, vol. 54, pp. 83–91, 2015.

[78] M.-Y. Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems,” *Comput. Commun.*, vol. 34, no. 1, pp. 107–117, 2011.

[79] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, “A survey of black hole attacks in wireless mobile ad hoc networks,” *Human-centric Comput. Inf. Sci.*, 2011.

[80] M. R. Babu and G. Usha, “A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET,” *Wirel. Pers. Commun.*, vol. 90, no. 2, pp. 831–845, 2016.

[81] D. Cerri and A. Ghioni, “Securing AODV: the A-SAODV secure routing prototype,” *IEEE Commun. Mag.*, vol. 46, no. 2, 2008.

[82] A. K. Mishra and B. Sahoo, “A modified adaptive-saodv prototype for performance enhancement in manet,” *Int. J. Comput. Appl. Eng. Technol. Sci.*, vol. 1, no. 2, pp. 444–47, 2009.

[83] T. Poongodi and M. Karthikeyan, “Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks,” *Wirel. Pers. Commun.*, vol. 90, no. 2, pp. 1039–1050, 2016.

[84] P. Sachan and P. M. Khilar, “Securing AODV routing protocol in MANET based on cryptographic authentication mechanism,” *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 5, p. 229, 2011.

[85] M. Patel and S. Sharma, “Detection of malicious attack in MANET a behavioral approach,” in *Proceedings of the 2013 3rd IEEE International Advance Computing Conference, IACC 2013*, 2013.

[86] G. J. Simmons, “Symmetric and Asymmetric Encryption,” *ACM Comput. Surv.*, 1979.

[87] T. Issariyakul and E. Hossain, “Introduction to Network Simulator 2 (NS2),” in *Introduction to Network Simulator NS2*, Springer, 2012, pp. 21–40.

[88] S. A. Jafar and A. Goldsmith, “Transmitter optimization and optimality of beamforming for multiple antenna systems,” *IEEE Trans. Wirel. Commun.*, 2004.

[89] R. Fotohi, S. Jamali, and F. Sarkohaki, “Performance Evaluation of AODV, LHC-AODV, OLSR, UL-OLSR, DSDV Routing Protocols,” *Int. J. Inf. Technol. Comput. Sci.*, vol. 5, p. 21, 2013.

[90] 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),” *Int. J. Adv. Res. Eng. Technol.*, 2013.

[91] J. A. Hanley and B. J. McNeil, “The meaning and use of the area under a receiver operating characteristic (ROC) curve.,” *Radiology*, 1982.

[92] Basu, Sandipan, "International Data Encryption Algorithm (Idea)–A Typical Illustration." *Journal of global research in Computer Science 2,* no. 7, pp. 116-118, 2011.

[93] Leong, M.-P., Cheung, O. Y. H., Tsoi, K. H., & Leong, P. H. W. (2000). A bit-serial implementation of the international data encryption algorithm IDEA. In Field- Programmable Custom Computing Machines, 2000 IEEE Symposium on (pp. 122– 131). IEEE.