IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

Contradiction Based Gray-Hole Attack Minimization for Ad-Hoc Networks

Saranya. R[1], Padmapriya. R[2]

Assistant Professor, School of Computer Studies, Rathnavel Subramaniam College of Arts and Science, Coimbatore, India[1]

Associate Professor, School of Computer Studies, Rathnavel Subramaniam College of Arts and Science, Coimbatore, India[2]

Abstract: The Mobile Ad-hoc Network (MANET) is a moveable wireless network that can transfer the information from source to destination. The recent research this network is widely used all around the wireless network because it does not require any fixed wired network to establish communication between the source and the destination. The major problem in MANET is black hole attack, a malicious node utilizes its routing protocol in order to announce itself for having the direct path to the destination node. The problem in open communication broadcasting the mobile ad-hoc network has some security limitations there are the option of information leakage in the wireless network. The propose system to identify and prevent the both blackhole & grayhole attack in MANET grayhole attack more than one node collude to each other hence this attack is more challenging to recognize. The main target of propose algorithm is to measure the impact of black hole attack and gray holeattack detection on the MANET's using secure algorithm combine with AODV routing protocol. The proposed system investigates the effects of the cooperative gray and black hole attack against AODV. The gray hole and black hole identification based on control packet algorithm. The Proposed method will combine secure Ad hoc On-demand Distance Vector (SAODV) with Elliptic Curve Cryptography (ECC) routing protocol. The experimental result shows the better performance compare with existing routing protocol.

Keywords: Mobile ad-hoc network, secure Ad hoc On-demand distance Vector, Elliptic Curve Cryptography, Ad hoc On-demand distance Vector

I. INTRODUCTION

MANETs are composed of autonomous nodes that are self-managed without any infrastructure. In this way, ad-hoc networks have a dynamic topology such that nodes can easily join or leave the network at any time. Basically MANETs are suitable for the areas where it is not possible to set up a fixed infrastructure. Since, the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. To sustenance this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and DSDV (Destination-Sequenced Distance-Vector). Each node also acts as a router to discover a path and forward packets to the correct node in the network. As MANETs lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Gray Hole attack. In the Gray Hole attack, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Gray Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface we simulated the Gray Hole attack node which is deliberately misbehaving, as well as a damaged node interface we simulated the Gray Hole attack.

I. OVERVIEW OF MANET NETWORK

Mobile Ad-Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. At the same time these nodes can act as host/router or both. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self-configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR etc.

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 2, February 2018

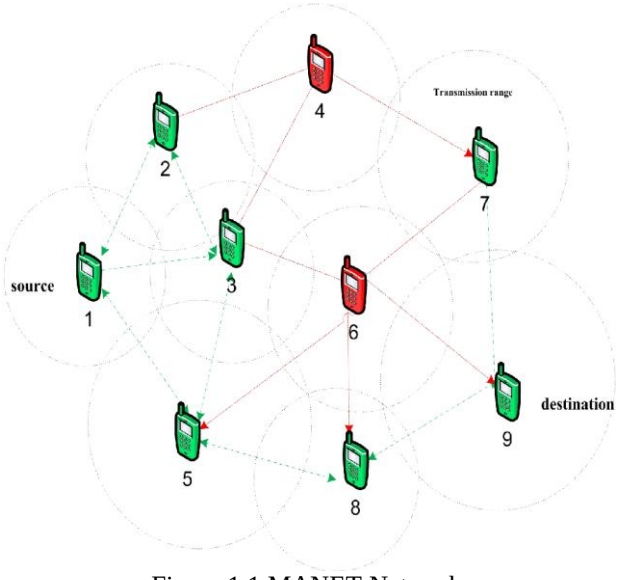

Figure 1.1 MANET Network

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DOS), selfish node misbehaving, impersonation attack is kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

II. ROUTING PROTOCOLS IN MANET

There are various routing protocols in MANET. In this section, we discuss the popular routing protocols in MANET. Before a mobile node wants to communicate with a target node, it should broadcast its present status to the neighbors. According to the mechanism the information is acquired, the routing protocols can be categorized into proactive, reactive and hybrid routing. An ad hoc routing protocol is a standard or convention way to control the nodes, that how nodes are decide to route packets between computing devices in a mobile ad hoc network. In ad hoc networks, nodes are not aware with the topology of their own networks. Instead, the nodes have to determine it. Normally, a new node announces its presence and listens for announcements broadcast by its neighbors. Each node can learns about others nearby nodes and how to reach them. In a wider sense, ad hoc protocol can also be used accurately, to mean an improvised and often impromptu protocol established for a specific purpose. The following is a list of some ad hoc network routing protocols.

Proactive Routing Protocol

The proactive routing is also known as table-driven routing protocol. In this routing protocol, mobile nodes broadcast their routing information to the neighbors periodically. Each node needs to maintain its routing table which records the adjacent nodes and reachable nodes the number of hops to reach to them. In other words, all of the nodes have to evaluate their neighborhoods as long as the network topology has changed. Therefore, the disadvantage of these routing protocols is that the overhead increases as the network size increases. However, the advantage is that network status can be immediately reflected if any malicious node joins the network. In a way Destination Sequenced Distance Vector (DSDV) routing protocol and Optimized Link State Routing (OLSR) Protocol, are some of the most familiar proactive routing protocols.

Reactive Routing Protocol

The reactive routing is also known as on-demand routing protocol. Unlike the proactive routing where node has information in advance, the reactive routing is simply started when a nodes desire to send data packets. The advantage is that the wasted bandwidth induced from the cyclically broadcast can be reduced. Nevertheless, this might also be the

fatal wound when there are any malicious nodes in the network environment. The disadvantage is that it leads to some packet loss. And Ad-hoc On-demand Distance Vector (AODV) routing protocol and Dynamic Source Routing (DSR) protocol are some of the most familiar reactive routing protocols. AODV is designed based on DSDV routing. AODV establishes route to the destination node when it is desired by the source node. It also maintains the routing path from source to destination node. One of the remarkable feature of AODV protocol is its use of destination sequence number designated to every route. Destination sequence number is generated by the destination node to include route information that is sent to the requesting node. Mobile nodes communicate to each other by sending Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) messages defined by AODV.

Whenever a source node desires to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination node is available or not. If there is no fresh route available, the route discovery process will be executed immediately. In this phase, the source node broadcasts the route request (RREQ) packet first. Then all intermediate nodes receive the RREQ packets, but only those nodes send the route reply (RREP) packet to the source node which have destination node information in their routing table. On the other hand, the route maintenance process is started when the network topology has changed or the connection has failed. The source node is informed by a route error (RERR) packet first. Then it utilizes the present routing information to decide a new routing path or restart the route discovery process to update the information in routing table.

Hybrid Routing Protocol

The hybrid routing protocol comes with the strength of proactive routing and reactive routing. Hybrid routing protocols are designed as a hierarchical or layered network framework. Initially, proactive routing is employed to completely gather the unfamiliar routing information, then reactive routing is used to maintain the routing information when topology changes. The familiar hybrid routing protocols are Zone Routing Protocol (ZRP) and Temporally-Ordered Routing Algorithm (TORA).

III. RELATED WORKS

Y.-C. Hu, et., al., "**Wormhole attacks in wireless networks**," 2006 As mobile ad hoc network applications are deployed, security emerges as a central requirement. In this paper, we introduce the wormhole attack, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. We present a general mechanism, called packet leashes, for detecting and, thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes. We also discuss topology-based wormhole detection, and show that it is impossible for these approaches to detect some wormhole topologies.

E. Gerhards-Padilla et., al., "**Detecting black hole attacks in tactical manets using topology graphs**," 2007. Black Hole Attacks are a serious threat to communication in tactical MANETs. In this work we present TOGBAD a new centralized approach, using topology graphs to identify nodes attempting to create a black hole. We use well-established techniques to gain knowledge about the network topology and use this knowledge to perform plausibility checks of the routing information propagated by the nodes in the network. We consider a node generating fake routing information as malicious. Therefore, we trigger an alarm if the plausibility check fails. Furthermore, we present promising first simulation results. With our new approach, it is possible to already detect the attempt to create a black hole before the actual impact occurs.

B. Kannhavong et., al., "**Nis01-2: A collusion attack against olsr-based mobile ad hoc networks**," 2006 Rapid advances in wireless networking technologies have made it possible to construct a Mobile Ad hoc Network (MANET) which can be applied in infrastructure less situations. However, due to their inherent characteristics, MANETs are vulnerable to various kinds of attacks which aim at disrupting their routing operations. To develop a strong security scheme to protect against these attacks it is necessary to understand the possible form of attacks that may be launched. Recently, researchers have proposed and investigated several possible attacks against MANET. However, there are still unanticipated or sophisticated attacks that have not been well studied. In this paper, we present a collusion attack model against Optimized Link State Routing (OLSR) protocol which is one of the four standard routing protocols for MANETs. After analyzed the attack in detail and demonstrated the feasibility of the attack through simulations, we present a technique to detect the attack by utilizing information of two hops neighbors.

W. Yu et., al., "**Hadof: defense against routing disruptions in mobile ad hoc networks**," 2005 HADOF is a set of mechanisms to protect mobile ad hoc networks against routing disruption attacks launched by inside attackers. First, each node launches a route traffic observer to monitor the behavior of each valid route in its route cache, and to collect the packet forwarding statistics submitted by the nodes on this route. Since malicious nodes may submit false reports, each node also keeps cheating records for other nodes. If a node is detected as dishonest, this node will be excluded from future routes, and the other nodes will stop forwarding packets for it. Third, each node will try to build friendship with other nodes to speed up malicious node detection. Route diversity will be explored by each to discover multiple routes to the destination, which can increase the chance of defeating malicious nodes who aim to prevent good routes from being discovered. In addition, adaptive route rediscovery will be applied to determine when new routes should be discovered. HADOF can handle various attacks and introduces little overhead to the existing protocols. Both analysis and simulation studies have confirmed the effectiveness of HADOF.

M. Mohanapriya and I. Krishnamurthi, "**Modified {DSR} protocol for detection and removal of selective black hole attack in {MANET}**," 2014. A black hole attack in ad hoc network refers to an attack by malicious nodes, which forcibly acquires the route from a source to destination by falsely advertising shortest hop count to reach the destination node. In this paper, we present a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. Selective black hole attack is a special kind of black hole attack where malicious nodes drop the data packets selectively. We proposed an Intrusion Detection System (IDS) where the IDS nodes are set in promiscuous mode only when required, to detect the abnormal difference in the number of data packets being forwarded by a node. When any anomaly is detected, the nearby IDS node broadcast the block message, informing all nodes on the network to cooperatively isolate the malicious node from the network. The proposed technique employs Glomosim to validate the effectiveness of proposed intrusion detection system.

R. H. Jhaveri et., al., "**Dos attacks in mobile ad hoc networks: A survey,**" 2012. MANETs have unique characteristics like dynamic topology, wireless radio medium, limited resources and lack of centralized administration; as a result, they are vulnerable to different types of attacks in different layers of protocol stack. Each node in a MANET is capable of acting as a router. Routing is one of the aspects having various security concerns. In this paper, we will present survey of common Denial-of-Service (DoS) attacks on network layer namely Wormhole attack, Blackhole attack and Grayhole attack which are serious threats for MANETs. We will also discuss some proposed solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols.

S. Banerjee., "**Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks**," 2008. The inherent features (such as-open medium, dynamically changing network topology, lack of centralized monitoring and management point, and lack of a clear line of defense) of the MANET make it vulnerable to a wide range of attacks. There is no guarantee that a communication path is free from malicious or compromised nodes which deliberately wish to disrupt the network communication. So, protecting the mobile ad-hoc network from malicious attacks is very important and challenging issue. In this paper, we address the problem of packet forwarding misbehavior and propose a mechanism to detect and remove the black and gray hole attacks. Our technique is capable of finding chain of cooperating malicious nodes which drop a significant fraction of packets.

N. Schweitzer et., al., "**Mitigating denial of service attacks in olsr protocol using fictitious nodes**," 2016. With the main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be vulnerable to various attacks. Over the years, emphasis has also been placed on improving the security of these networks. Different solutions have been proposed for different types of attacks, however, these solutions often compromise routing efficiency or network overload. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Through extensive experimentation we demonstrate that 1) the proposed protection prevents more than 95% of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non- discernable. Lastly, we suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

A. Laouiti, et., al., "**Quantitative evaluation of the cost of routing protocol olsr in a vehicle ad hoc network (vanet)**," 2008. In this paper, we study the channel occupation induced by the OLSR [1] proactive routing protocol used in a linear Vehicular Ad hoc Network (VANET). Unlike previous studies which usually use simulations to evaluate the overhead of routing protocols, we derive a simple analytical model to carry out this evaluation. Moreover, we do not evaluate the total overhead induced by the routing protocol as is usually proposed, but for a given node we compute the channel occupation induced by the routing protocol. This paper provides a quantitative approach to

evaluating the cost of a proactive routing protocol in a linear Vehicular Ad hoc Network as a function of several parameters such as the frequency of the control messages, the density of the vehicles, the propagation range of the control messages and the carrier sense area.

T. Chen et., al.,, "**Trusted routing for vanet**" 2009. Trust establishment in VANET is a particularly challenging task due to the lack of infra-structure, openness of wireless links and the usually highly dynamic network topology. To overcome these difficulties, we propose a trusted routing framework that provides message authentication, node-to-node trust and routability verification, without online assistance of Certificate Authorities (CA). Our approach prevents identity impersonation, false link availability indication by compromised nodes as well as some of routing protocol specific misbehaviours. By applying this framework to the Optimised Link State Routing Protocol (OLSR), we demonstrate how this mechanism can be used to establish trusted routes.

J. Santa, et., al., "**Assessment of VANET multi-hop routing over an experimental platform**," 2009. Evaluation of vehicular ad-hoc networks (VANETs) over real environments is still a remaining issue for most researchers. There are some works which carry out performance tests to evaluate the communication channel according to physical and MAC conditions. Only a few works deal with multi-hop experimentation in this field, and practically none tests multihop protocols. In this paper, an integral VANET testbed is evaluated, using 802.11b and a multi-hop network managed by the Optimized Link State Routing protocol (OLSR). Up to four vehicles are used to study the VANET performance over different traffic environments and different metrics are considered to analyse the results in terms of delay, bandwidth, packet loss and distance between nodes. Furthermore, a deeper analysis is carried out to track the routes followed by packets end to end. Since a routing protocol is used, results differ from traditional one-hop and static-route tests, presenting a more realistic study.

H. Deng et., al., **"Routing security in wireless ad hoc networks**," 2002. A mobile ad hoc network consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability. Routing plays an important role in the security of the entire network. In general, routing security in wireless MANETs appears to be a problem that is not trivial to solve. In this article we study the routing security issues of MANETs, and analyze in detail one type of attack the "black hole" problem that can easily be employed against the MANETs. We also propose a solution for the black hole problem for ad hoc on-demand distance vector routing protocol.

T. Poongodi and M. Karthikeyan, "**Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks**," 2016. Black hole attack refers an attack by single or more number of malicious nodes which forcibly captures the route from source to destination by sending reply with largest sequence number and smallest hop count. In this paper, a novel technique using Localized Secure Architecture for MANET (LSAM) routing protocol is proposed to detect and prevent co-operative black hole attack. Security Monitoring Nodes (SMNs) would be activated only if the threshold value is exceeded. If malicious nodes are detected, other SMNs in its proximity area are intimated to isolate the malicious nodes. Network simulator tool is implemented to analyze the network performance of different scenarios with various number of nodes. Packet delivery ratio (PDR), routing overhead, control overhead, packet drop rate, throughput and end-to-end delay (EED) are the factors taken into consideration for performance analysis and it is shown that the proposed protocol is more secured and efficient. PDR is being increased by 27 % in the presence of 40 % misbehaving nodes, while it increases the percentage of overhead on proposed routing protocol from 1 to 4 %. EED is greatly reduced from 0.9 to 0.3 % in LSAM.

S. Djahel et., al., "**An acknowledgment based scheme to defend against cooperative black hole attacks in optimized link state routing protocol**" 2008 In this paper, we address the problem of cooperative black hole attack, one of the major security issues in mobile ad hoc networks. The aim of this attack is to force nodes in the network to choose hostile nodes as relays to disseminate the partial topological information, thereby exploiting the functionality of the routing protocol to retain control packets. In optimized link state routing (OLSR) protocol, if a cooperative black hole attack is launched during the propagation of topology control (TC) packets, the topology information will not be disseminated to the whole network which may lead to routing disruption. In this paper, we investigate the effects of the cooperative black hole attack against OLSR, in which two colluding MPR nodes cooperate in order to disrupt the topology discovery. Then we propose an Acknowledgment based technique that overcomes the shortcomings of the OLSR protocol, and makes it less vulnerable to such attacks by identifying and then isolating malicious nodes in the network. The simulation results of the proposed scheme show high detection rate under various scenarios.

J. M. Chang et., al., "**Defending against collaborative attacks by malicious nodes in manets: A cooperative bait detection approach**," 2015 Wireless networks are computer networks that are not connected by cables of any kind.

The use of wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. Wireless networks are susceptible to many attacks. One such specific attack is a blackhole attack in which malicious node falsely claiming itself as having the fresh and shortest path to the destination. This paper attempts to resolve this issue by designing a dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. Proposed system helps us in defending against the blackhole attack without any requirement of hardware and special detection node.

A. D. Patel and K. Chawda "**Dual Security Against Grayhole Attack in MANETs**," 2015 The most critical issue related to the mobile ad hoc networks is the security. Due to various characteristics, MANET is likely to be exposed to the Grayhole attack. This type of attack tends to degrade the network performance by falsifying the route and dropping the packets. The Grayhole attack may take place during the route discovery time as well as during the data transmission time. In this paper, we provide a solution which would mitigate the Grayhole attack during the route discovery phase as well as during the data transmission phase. Our solution detects the attack taking place during any of the two phases.

G. S. Bindra, et., al., "**Detection and removal of co-operative blackhole and grayhole attacks in manets**," 2012 A MANET, by definition, comprises of nodes which are mobile. It has a dynamic topology and lacks a central controlling entity. These features along with undefined and unsecure boundaries make its security a very challenging issue. Blackhole and grayhole attacks can in fact seriously compromise the performance of a critical infrastructure like a MANET. In this paper, we propose a mechanism to detect and remove the blackhole and grayhole attacks. The solution we are proposing tackles these attacks by maintaining an Extended Data Routing Information (EDRI) Table at each node in addition to the Routing Table of the AODV protocol. The mechanism is capable of detecting a malicious node. It also maintains a history of the node's previous malicious instances to account for the gray behavior. Refresh packet, Renew Packet, BHID Packet, Further request and Further reply packets are also used in addition to the existing packets (RREQ and RREP). Our technique is capable of finding chain of cooperating malicious nodes which drop a significant fraction of packets.

IV. CONCLUSION

The Mobile Ad-Hoc Network (MANET) is a moveable wireless network that can transfer the information from source to destination. The recent research this network is widely used all around the wireless network because it does not require any fixed wired network to establish communication between the source and the destination. The major problem in MANET is black hole attack, a malicious node utilizes its routing protocol in order to announce itself for having the direct path to the destination node. The problem in open communication broadcasting the mobile ad-hoc network has some security limitations there are the option of information leakage in the wireless network. The propose system to identify and prevent the both blackhole & grayhole attack in MANET grayhole attack more than one node collude to each other hence this attack is more challenging to recognize. The main target of propose algorithm is to measure the impact of black hole attack and gray hole attack detection on the MANET's using secure algorithm combine with AODV routing protocol. The proposed system investigates the effects of the cooperative gray and black hole attack against AODV. The gray hole and black hole identification based on control packet algorithm. The Proposed method will combine secure Ad hoc On-demand distance Vector (SAODV) with Elliptic Curve Cryptography (ECC) routing protocol. The experimental result shows the better performance compare with existing routing protocol.

REFERENCES

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370–380, Feb 2006.
[2] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke, and J. Tolle, "Detecting black hole attacks in tactical manets using topology graphs," in 32nd IEEE Conference on Local Computer Networks (LCN 2007), Oct 2007, pp. 1043–1052.
[3] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "Nis01-2: A collusion attack against olsr-based mobile ad hoc networks," in IEEE Globecom 2006, Nov 2006, pp. 1–5.
[4] W. Yu, Y. Sun, and K. J. R. Liu, "Hadof: defense against routing disruptions in mobile ad hoc networks," in Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., vol. 2, March 2005, pp. 1252–1261 vol. 2.
[5] M. Mohanapriya and I. Krishnamurthi, "Modified {DSR} protocol for detection and removal of selective black hole attack in {MANET}," Computers & Electrical Engineering, vol. 40, no. 2, pp. 530 – 538, 2014.
[6] 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, Jan 2012, pp. 535–541.
[7] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. E. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks." in International conference on wireless networks, vol. 2003, 2003.
[8] S. Banerjee, "Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks," in proceedings of the world congress on engineering and computer science, 2008, pp. 22–24.
[9] N. Schweitzer, A. Stulman, A. Shabtai, and R. D. Margalit, "Mitigating denial of service attacks in olsr protocol using fictitious nodes," IEEE Transactions on Mobile Computing, vol. 15, no. 1, pp. 163–172, Jan 2016.

[10] J. Haerri, F. Filali, and C. Bonnet, "Performance comparison of AODV and OLSR in VANETs urban environments under realistic mobility patterns," in Med-Hoc-Net 2006, 5th IFIP Mediterranean Ad-Hoc Networking Workshop, June 14-17, 2006, Lipari, Italy, Lipari, ITALY, 06 2006.
[11] A. Laouiti, P. Muhlethaler, F. Sayah, and Y. Toor, "Quantitative evaluation of the cost of routing protocol olsr in a vehicle ad hoc network (vanet)," in Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, May 2008, pp. 2986–2990.
[12] T. Chen, O. Mehani, and R. Boreli, "Trusted routing for vanet," in Intelligent Transport Systems Telecommunications,(ITST),2009 9th International Conference on, Oct 2009, pp. 647–652.
[13] J. Santa, M. Tsukada, T. Ernst, O. Mehani, and A. F. Gómez-Skarmeta, "Assessment of VANET multi-hop routing over an experimental platform," International Journal of Internet Protocol Technology, vol. 4,no. 3, Sep. 2009.
[14] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70–75, Oct 2002.
[15] 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.
[16] T. Poongodi and M. Karthikeyan, "Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks," Wireless Personal Communications, vol. 90, no. 2, pp. 1039–1050, 2016.
[17] S. Djahel, F. Nait-Abdesselam, and A. Khokhar, "An acknowledgmentbased scheme to defend against cooperative black hole attacks in optimized link state routing protocol," in 2008 IEEE International Conference on Communications, May 2008, pp. 2780–2785.
[18] J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao, and C. F. Lai, "Defending against collaborative attacks by malicious nodes in manets: A cooperative bait detection approach," IEEE Systems Journal, vol. 9, no. 1, pp. 65–75, March 2015.
[19] A. D. Patel and K. Chawda, Dual Security Against Grayhole Attack in MANETs. New Delhi: Springer India, 2015, pp. 33–37
[20] G. S. Bindra, A. Kapoor, A. Narang, and A. Agrawal, "Detection and removal of co-operative blackhole and grayhole attacks in manets," in System Engineering and Technology (ICSET), 2012 International Conference on, Sept 2012, pp. 1–5.