International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Diminution of MANET Attacks by HOOSC Scheme

Amanpreet Kaur[1], Manjot Kaur Sidhu[2]

[1]Research scholar, CSE, Chandigarh Group of College, Gharuan, Mohali, Punjab, India

[2]Associate Professor, CSE, Chandigarh Group of College, Gharuan, Mohali, Punjab, India

Abstract: ***In this paper, an Ad-Hoc On Demand Distance Vector (AODV) protocol along with HOOSC scheme is put forward which encrypts the message to be sent and provides security for consistent routing. HOOSC algorithm allows a sender in the IBC (identity based cryptography) to send a message to a receiver in the PKI (public key infrastructure). Security in Mobile Ad-Hoc Network is an important concern for the proper functionality of network. During routing, MANET often suffers various security attacks because of the absence of clear defense algorithm. But the attacks, which can bring a large damage to MANET is called Black Hole and Grey Hole attacks. These attacks can distract the process of routing because of their direct attack on the router. Hence, several energy efficient routing algorithms and protocols are used in the previous works which are not capable efficiently to face these attacks. So HOOSC scheme is used which is very suitable to provide the security solution. In this work, the comparative analysis has been carried out by using AODV protocol without security, Message Digest algorithm and HOOSC Scheme along with AODV protocol. The simulated results show HOOSC gives better and enhanced results to mitigate the attacks in MANETs when it get modeled with HOOSC Scheme.***

Keywords: Mobile Ad-Hoc Network (MANET), Ad-Hoc On Demand Distance Vector (AODV) Protocol, Signcryption, Message Digest (MD5), HOOSC Scheme, Black hole Attack, Grey hole Attack**.**

1. Introduction

Mobile Ad-Hoc Network (MANET) is a network which is purely wireless in nature having the properties to configure themselves continuously. These networks are infrastructure-less networks comprising of various nodes or devices which are mobile in nature. These devices are connected to each other in a wireless manner. MANET is an independent network in which the nodes are deployed in a random manner. The speed of nodes is not same and hence, the link of nodes with other devices changes more often. The primary issue in the construction of MANET is that each device has to be equipped properly for the continuously routing of data. These types of devices are connected with each other directly or with the help of internet. The concept of MANET is different from other wireless sensor networks or wireless networks because of its multihop routing technique. In this concept, the nodes always use an intermediate node for the process of communication. This intermediate node may or may not be exited within the communication range. Hence, the communication in MANETS depends entirely on the mutual understanding between the nodes [1]. Due to this, each and every individual node in mobile ad hoc networks exhibit the role of router as well as host. There are various advantages of

MANET which are explained as follows:

A. Self-Configuring and Infrastructure Independent Networks

MANET is composed of thousands of nodes which are arrange themselves or can configure themselves again and again. These networks do not depend upon the infrastructure of mobile devices. Due to this, the central administrator is also not requires in MANETs.

B. Routing Scheme

The concept of multihop routing scheme is also act as an efficient role. Each node in MANET has to be act as a host and router for the processing of information. The node which acts as a host or router is also known as intermediate node.

C. Topology Type

MANETs exhibit the Dynamic topology scheme because of the behavior of nodes. The nodes can connect or disconnect their selves from the network at any time [18]

D. Energy Efficiency Problem

As the nodes in ad-hoc networks are integrated with limited or restricted battery storage, hence for this reason, while processing the information from one source node to intermediate node or destination node, the life of sensor as well as ad hoc network reduces. This restricts the processing power of mobile nodes. Hence, energy efficiency is one of important concerns in MANETs [18].

For the forwarding of data and to provide a route to the information or data, various routing protocols are used. But, for the proper routing, a standard routing protocol is put forward which acts efficiently in a decentralized as well as in a random environment. Ad-Hoc On Demand Distance Vector (AODV) Protocol is one of the energy effective protocol which is used to provide the multihop routing scheme in MANETs. This protocol is a pure reactive protocol which sets up a proper route between the source and the destination under the discovery and maintenance of provided route [3]. MANETs face various minor or major security attacks during the routing among which Black Hole and Grey Hole attacks are one of the most dominant attacks which disturb the whole

of the performance of network. A harmful or malicious node in black hole attack acquires route from the source to destination and crashes all the received packets. On the other hand, the malicious node transforms its behavior from a standard node to a harmful or malicious node [4].

This paper explores the existing mechanisms and applies HOOSC Scheme along with AODV protocol to minimize the attacks of black hole and grey hole. Also, a comparative analysis has also been carried out between MD5 algorithm, HOOSC scheme and by using AODV protocol without security. The results have been taken out practically by using NS-2 simulator.

The whole of the paper is ordered as follows. Section II describes the related work, section III explains the concept of proposed protocol AODV, section IV describes the attacks i.e. grey hole and black hole attacks and section V focuses on HOOSC Scheme. Section VI presents the proposed methodology, Section VII consists of simulated results and discussion part and Section VIII discusses on conclusion and future scope of the proposed work.

2. Related Work

The complication issues regarding security threat in MANETs has become a vital problem which has to be minimized in order to increase the efficiency of network. Many protocols, algorithms and routing mechanisms have been proposed in various works for minimizing the effect of attacks in MANETs. In the year 2000, the observation-based techniques was proposed in [5] for the detection of malicious nodes and reporting of malicious nodes to the main node or source node. The mitigation has also been reduced by the use of payment schemes in which the researchers investigated the means to depress the self-centered routing activities [15]. In the year 2002, a mechanism is applied to shelter the network from black hole attacks. The protocol used was AODV protocol. The authors proposed a mechanism in which the source node again sends the route request to the neighbor node of an intermediate node after the receiving of route reply. This is done to check that whether the route exist in practical manner or not [7].

In [19] [24], authors proposed a solution for the detection of malicious nodes by using PEAK value. The source node transmits a catalog of malicious or harmful nodes with the RREQ packets. This PEAK value is considered as the highest probable value of sequence numbers that any route can reply in the existing session. The node having RREP packet sequence number larger than that of PEAK value is perceived as a malicious node. The packet RREP coming from the malicious node is manifested as DO_NOT_CONSIDER and then forwarded in the reverse path. But in [20], the source node can never broadcast the RREP to repeal path to avoid overhead. The intrusion detection system has also been proposed by Fuzzy logic. The traffic within the network for the detection of black and gray hole has been observed by IDS in [21]. The AODV protocol which is secure in nature is put forward in 2012 for the mitigation of black hole attack by getting feedback from other nodes before the transmission of data.

In the year 2007, a mechanism has been put forward for the detection of gray hole attack. The detection of gray hole attack engages proactively invoking of joint and distributive algorithms involving neighbors. This concept depends upon the threshold cryptography [12].

3. AODV Protocol

Ad-hoc On demand Distance Vector (AODV) routing protocol is a pure reactive protocol which created or establishes a proper route for the transference of information or data between the source and destination. The working of AODV protocol is separated into two phases named as Route discovery and Route maintenance phase [3].

a. Route Discovery

The implementation of this phase is put forward during the deficit of a valid route. When there exists a route which is invalid or not properly valid for the process of routing then this phase is used by the AODV protocol. During this phase, the source node or the initiated node broadcasts a message which is called Route Request (RREQ) Packet among the neighboring nodes. The reply message is sent by the destination or intermediate node in the form of Route Reply (RREP) Packet. This node replies only in the condition when it has a fresh or a new route to the destination node. After this, the link gets established in between the source as well as destination node [20] [19].

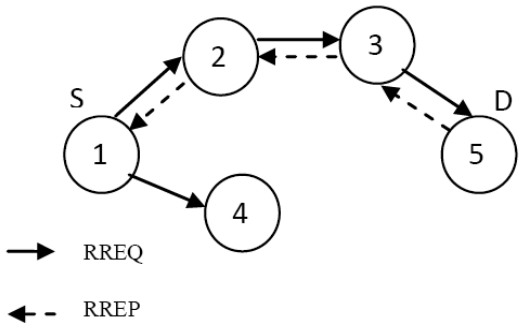

Figure 1: Route Discovery in AODV Protocol [4]

Figure 1 clearly shows the concept of discovery of route in AODV protocol by the use of message like RREQ and RREP packets. The S shows the source node and D shows the destination node. According the figure, the node 1 i.e. source node transmits or broadcasts RREQ packets to all of its neighbor nodes i.e. node 2 and node 4. Then again, the nodes 2 and 4 also broadcast the message to their neighboring nodes i.e. node 3 and the node neighbor to node 4.

The process repeating itself until the source node receives a RREQ packet message from the destination or any of intermediate nodes. On receiving the message RREQ packet, the node 5 which is a destination node responds. Due to this, the route get established between the node 1 and node 5 i.e. source and destination node for the transference of information via nodes 2 and 3 which act as intermediate nodes.

b. Route Maintenance

After the establishment of route from the source to destination, this phase named Route Maintenance phase comes in action for the proper and efficient route of data from the source to destination node. When any type of malfunctioning of nodes within a network detected then, the message Route Error Message (RERR) Packet is passed to all the nodes inside the network. This message also gets broadcasted when any link breakage or failure of link detection takes place.

The nodes repeatedly broadcast the message to their antecedent nodes till the message reaches the main or source node [4].

4. Black Hole and Grey Hole Attack

The two major types of security attacks faced by MANET are Black Hole and Gray Hole attacks which restricts the flow of packets from the source to destination node. The discussion on these two attacks is explained as follows.

a. Black Hole Attack

The attacks to sensor as well as Ad-Hoc networks are very common because of the deployment of random and arbitrary nodes which are dynamic in nature. The independent behavior of these nodes is vulnerable to many attacks which suppressed the efficiency of network. Because of the haphazard nature of nodes positioned in MANETs, the network gets much susceptible to various security threats and attacks which reduce the lifetime of a network. Among various security attacks, Black Hole and Grey Hole attacks are the most striking and prominent attacks in MANET.

In the case of black hole attack, the node which is malicious in nature attains or accesses the main route by providing the facility of shortest route between source node to destination node. The source node get tempted by this malicious node which provides the bogus sequence number and hop count during the broadcasting of RREP packet for the shortest route [13] [19].
The malicious or harmful node sends the RREP packet to the source node after the receiving of RREQ packet form it in a very fast manner without any inspection from the destination node. This RREP packet consists of fake or bogus sequence number and hop count. Hence, by doing this, the shortest path is created between the source and malicious node rather than source and destination node and the source node transmits all the useful data to the malicious node. After this, the malicious node drops the useful data and does various attacks like denial-of-service attack and eavesdropping [18].

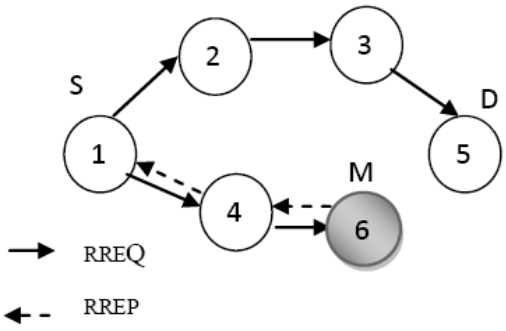

Figure 2: Black hole attack [4]

Figure 2 shows the process of black hole attack in MANETs where the node 6 which is a malicious node sends the data rapidly to the source node in the form of RREP packet than that of destination node after the receiving of RREQ packet. On receiving the RREP packet from the malicious node, the node 1 i.e. source node sends whole of the data to this malicious node and hence, all the data gets trapped in this malicious node [25] [22].

b. Gray Hole Attack

The concept of grey hole attack is differ from black hole attack in some of the aspects. In gray hole attack, some of the packets get dropped having a little probability. The gray hole is very difficult to detect because the malicious node changes its behavior from malicious to normal or standard behavior. The malicious node drops the packets coming from the source node while forwarding all the packets to destination node [23] [25].

5. HOOSC Scheme

An efficient HOOSC scheme is a scheme which allows a sender in the IBC (identity based cryptography) to send a message to a receiver in the PKI (public key infrastructure). It consists of the following five algorithms. A generic HOOSC scheme is composed of five algorithms which are explained as follows [26].

a. SETUP

Setup phase is an algorithm which is probabilistic in nature and run via PKG which considers input as a constraint of security k. It gives an output a master top secret key msk and the scheme factor params that comprise of a master public key which is abbreviated as mpk.

b. IBC-KG

The main purpose of this algorithm is to generate a key algorithm for the users of IBC. The main user put forwards an identity I D to its PKG. The PKG figure out the equivalent secret key sk and sends it to the user in a protected way. Take into consideration the user's public key pk is identity I D. This type of key does not need a digital certificate.

c. PKI-KG

This algorithm is implemented to generate a key for PKI users. Then, user selects a secret key which is demoted as sk

and issues the a new public key pk. This public key needs for a digital certificate which is sign by its CA.

d. Off-Signcrypt

This is a probabilistic offline signcryption algorithm run by a dispatcher that obtains as participation in the system stricture param, a publisher's private key sks and a recipient's public key pkr , and outputs an offline signcryption δ.

e. On-Signcrypt

On-Signcrypt is a probabilistic signcryption algorithm which is also an online algorithm. This algorithm is run by a correspondent which takes as an input system constraints, a message named as m and an offline signcryption referred to as δ, and gives an output as a full signcryption ciphertext σ [26].

f. Unsigncrypt

Unsigncrypt is a probabilistic signcryption algorithm which is run by the receiver which takes as an input cipher text, sender public key, and receiver private key and gives output in the form of plaintext.

6. Proposed Methodology

To provide the security and improvement in the infrastructure of MANET, a fresh scheme has been applied called HOOSC Scheme along with an efficient routing protocol AODV. The concept works on the principal of multihop routing technique in which the data or information can be sent to the destination node from the source node by the use of some of the intermediate nodes.

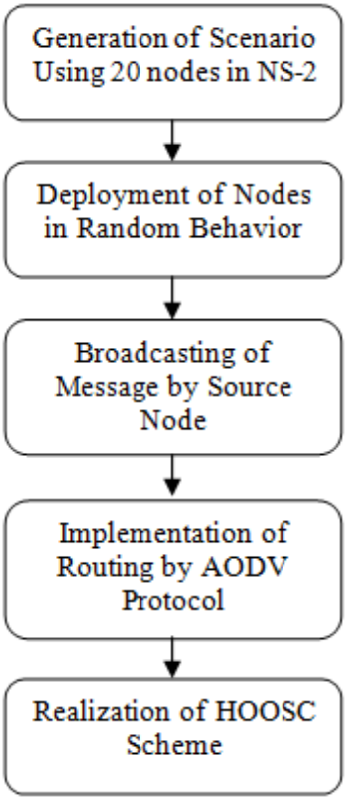

Figure 3: Flow of Work

The information to be sent to the destination node has to be encrypting first and then the source node sends the information. By applying this encryption to the data or information to be sent, the malicious node become unable to retrieve the information stored in the packets.

The phase 1 is the generation of scenario phase which is generated by the use of simulator NS-2 where 20 nodes are used. In the phase 2 the deployment of nodes is done by the use of random behavior i.e. in an ad hoc style which is arbitrary in shape. The nodes in this phase can also be showed haphazard behavior. The source node broadcasts the message or information in the phase 3 and the AODV protocol is applied to the message or information in order to provide the security to the routing scheme in the phase 4. Then, to provide security to the transmitted messages, HOOSC Scheme is applied which encrypts the message and adds the digital signature to it in order to avoid the attacks and to minimize them in the final phase.

7. Simulation Results and Discussion

In this section, the results have been carried out by the implementation of AODV protocol with HOOSC Scheme. A comparative analysis also been taken out by using AODV protocol without security, MD5 algorithm and HOOSC Scheme along with AODV algorithm. All the simulations been done on NS-2 simulator.

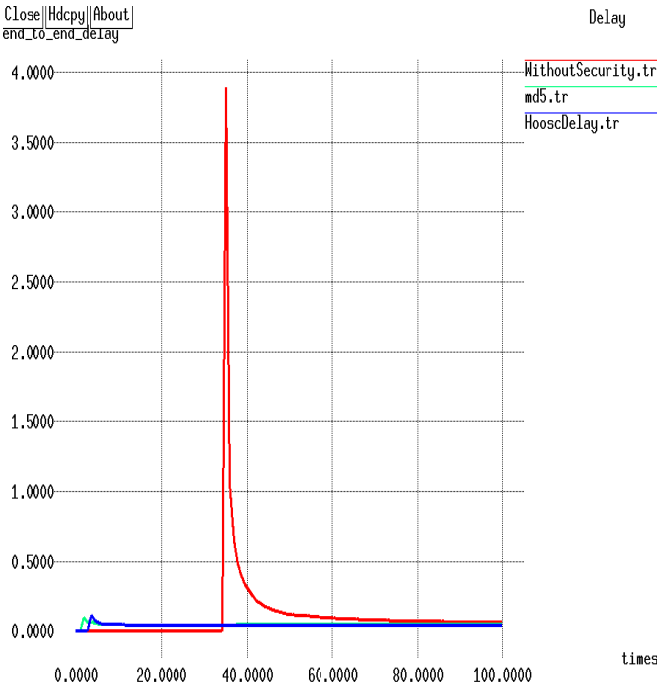

Figure 4: End to end delay

Figure 4 shows the end to end delay between the source node and destination node whiles the transference of information or messages. It is clearly shows that the HOOSC Scheme is better as compared to traditional ones.

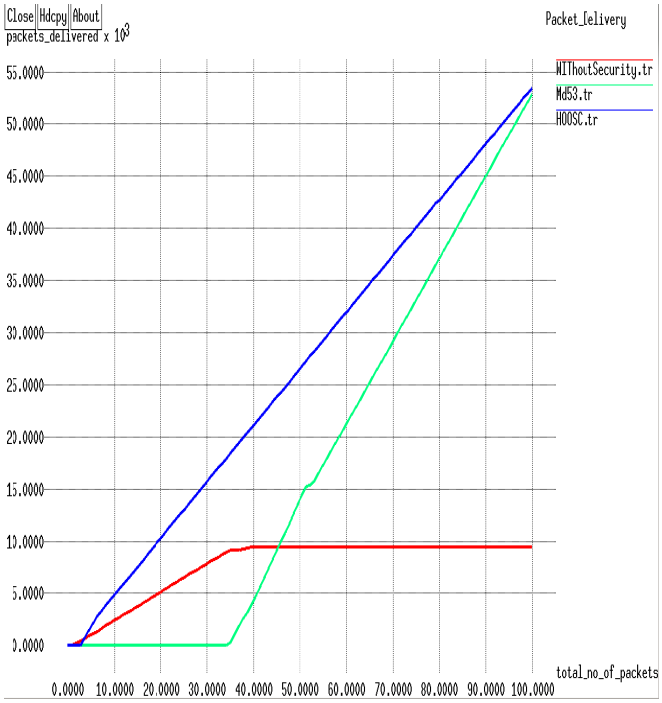

Figure 5: Packet Delivery Ratio

Figure 5 discusses the packet delivery ratio of nodes. It can be shown that the delivery of packets is excellent in HOOSC Scheme despite the other two algorithms.

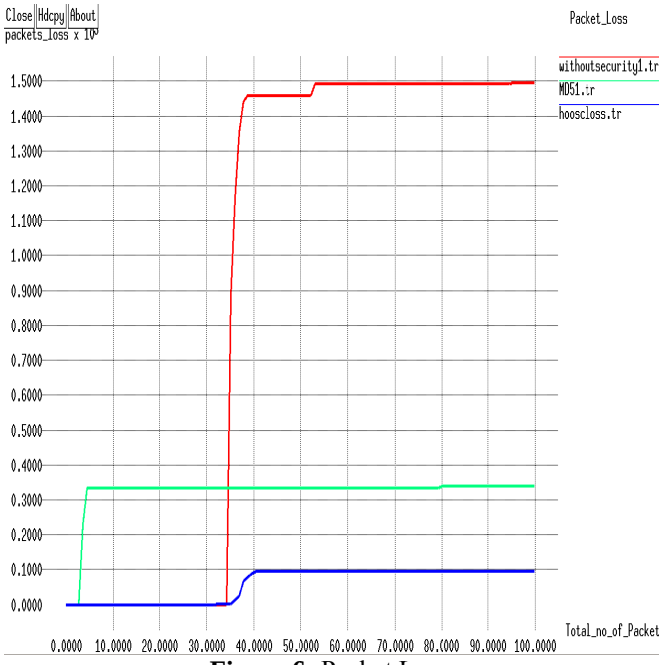

Figure 6: Packet Loss

Figure 6 describes that the loss of packets in HOOSC Scheme occur less than that of MD5 algorithm and when AODV protocol get used without security. Hence, HOOSC Scheme is more efficient and effective in the delivery of packets by minimizing the loss of packets.

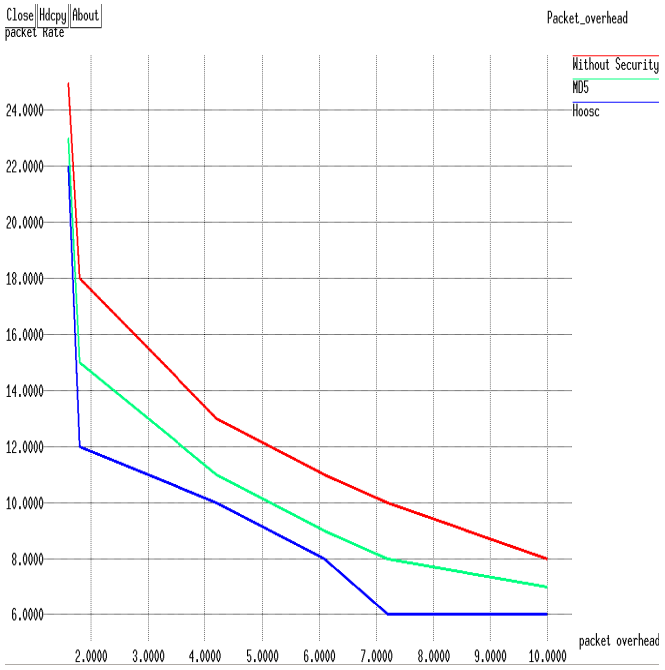

Figure 7: Packet Overhead

The overhead of packets while transferring the information from source node to destination node is shown in Figure 7. The graphical representation describes the behavior of HOOSC Scheme in which less overhead occurs.

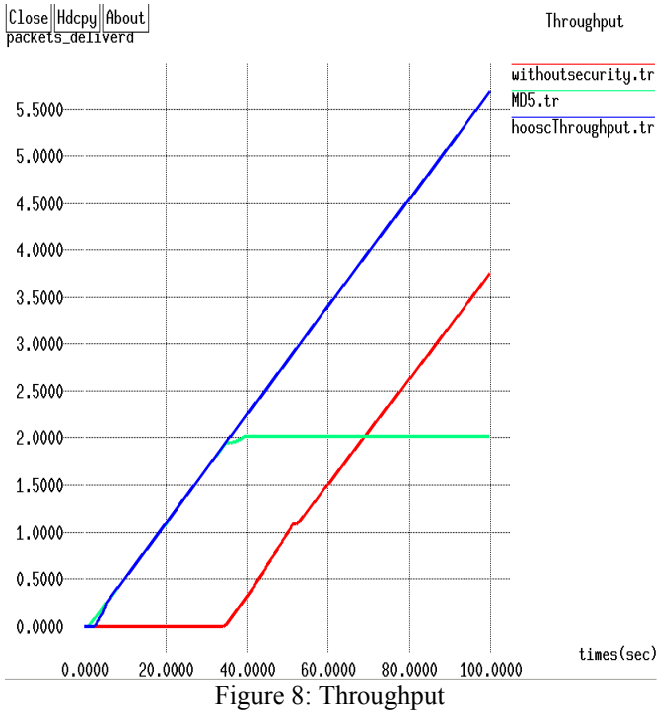

Figure 8: Throughput

Figure 8 represents the throughput of proposed HOOSC algorithm as compared to conventional ones. As shown in figure, the throughput provided by proposed HOOSC Scheme is much more efficient than that of AODV Protocol without security and by using MD5 algorithm.

8. Conclusion and Future Scope

In this paper, HOOSC scheme is used that provide more security and the comparative analysis of three different

algorithms has been carried out to find the most efficient and effective protocol used for the transference of information from source to destination node. The analysis has been taken out among MD5 algorithm, HOOSC Scheme and AODV protocol without security. In AODV protocol, the discovery of route is vulnerable to various threats like Black Hole and Gray Hole attacks. Hence, to diminution of these attacks, the HOOSC Scheme is implemented mainly to provide the security to the packets transmitted. The results in this paper revealed that the HOOSC Scheme outperforms the conventional schemes and algorithms in various aspects and parameters. With HOOSC scheme, it provides more security solutions and parameters like end to end delay decreases, packet delivery ratio increases.

In future work we can improve the performance by using PGP (Pretty Good Privacy) security protocol instead of AODV protocol along with HOOSC scheme with minimum delay & overhead and maximum Packet Delivery Ratio.

References

[1] IETF MANET work group. http://www.ietf.org/dyn/wg/charter/manet- charter.html
[2] F.Lilieblad, O.Mattsson, P.Nylund, D.Ouchterlony, "A. Roxenhag. Mad-hoc AODV Implementation and Documentation" http://mad-hoc.fiyinglinux.net
[3] C. E Perkins and E. M. Royer (1999), "Ad-hoc On-Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp-90-100.
[4] C. Lohi and S.K. Sharma "A Survey of Mitigation Techniques to Black Hole Attack and Gray Hole Attack in MANET", International Journal Computer Technology and Applications, 5(2), 560-567
[5] S. Marti, T. Guili, K. Lai, and M. Baker (2000), "Mitigating routing misbehavior in mobile ad hoc networks" ,In Proceedings of MOBICOM 2000, pp. 255-265.
[6] David B. Johson, David A. Maltz and Josh Broch (2001), "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad-Hoc networks", in Ad-hoc Networking, Edited by Charles E. Perkins, Chapter-5, pp-139-172, Addison-Wesley
[7] H. Deng, H. Li, and D.P. Agrawal (2002), "Routing security in wireless ad hoc networks," IEEE Communications Magazine, Vol. 40, No. 10.
[8] H. Deng; W. Li; D. Agrawal (2002) "Routing Security in Wireless Ad-Hoc Networks" Communications Magazine, IEEE, 70 - 75.
[9] H. Deng, H. Li, and D.P. Agrawal, (2002),"Routing security in wireless ad hoc networks," IEEE Communications Magazine, Vol. 40, No. 10.
[10] I. D. Chakeres and E. M. Belding-Royer(2002), The Utility of Hello Messages for Determining Link Connectivity in Proceedings of the 5th International Symposium on Wireless Personal Multimedia Communications (WPMC), pages 504. 508, Honolulu, Hawaii.
[11] S. Lee, B. Han, and M. Shin, (2003), "Robust Routing in Wireless Ad Hoc Networks," 2002 Int'l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.
[12] M. Jackobsson, J. Hubaux, and L. Buttyan, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks," In Proceedings of Financial Crypto.
[13] Y.C. Hu; A. Perrig, (2004), "A Survey of Secure Wireless Ad Hoc Routing [J]", IEEE Security and Privacy, 2(3), 28-39.
[14] Humaira Ehsan and Zartash Afzal Uzmi, "Performance Comparison of Ad Hoc Wireless Network Routing Protocols," Proceedings of INMIC 8th International, 24-26 Dec. 2004, pp-457- 465
[15] Jaydip sen et. al (2007),"A Mechanism for Detection of Gray Hole Attack in Mobile AD Hoc Networks" ICICS, IEEE.
[16] Bala A., Bansal M. and Singh J.(2009), "Performance Analysis of MANET under Blackhole Attack", In Proc. of First International Conference on Networks &Communications, pp. 141–145.
[17] Akanksha Saini and Harish Kumar(2010), "Comparison between Various Black Hole Detection Techniques in MANET", In Proc. of National Conference on Computational Instrumentation, pp. 157-161.
[18] Rajiv Ranjan, Naresh Trivedi and Anoop Srivastava (2011), "Mitigating of Black Hole Attack in Manets", VSRD International Journal of Computer Science and Information Technology, 1(2), 53-57.
[19] S. J. Patel et.al. (2012),"A Novel Approach to Gray-hole and Black-hole Attacks in Mobile Ad-hoc Networks" Second International Conference on Advanced Computing & Communication Technologies,IEEE, Pp 556-560.
[20] M. Wahengbam and N. Marchang, (2012),"Intrusion Detection in MANET using Fuzzy Logic", IEEE, pp. 456-460.
[21] Rajesh Yerneni and A.K. Sarje (2012), "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks" ICCCNT', IEEE, pp. 248-252.
[22] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, (2012),"DoS Attacks in Mobile Ad- hoc Networks: A Survey", In Proc. Of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), pp.535-5 41.
[23] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala (2012),"A Novel Approach for Grayhole and Blackhole Attacks in Mobile Ad-hoc Networks", In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS),, pp.556-560
[24] R. H. Jhaveri, (2013), "MR-AODV: A Solution to Mitigate Black-hole and Gray-hole Attacks in AODV Based MANETs" Third International Conference on Advanced Computing & Communication Technologies, IEEE, Pp. 254-260.
[25] K.Mahalakshmi et.al. (2013), "Intrusion Detection System Based MANET Security against Selective Black Hole Attacks" International Journal of Research in Computer Engineering and Electronics.
[26] Li., F., and Xiong., P.,(2013), "Practical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things", IEE Sensors Journal, vol.13, No. 10.

Author Profile

Amanpreet Kaur completed her bachelor of technology degree in 2012 from lovely professional university and master of technoloy in Computer sciene & engineering in 2014 from Chandigarh Groups of College, Gharuan. She has attended various research seminar. Her research interest area are in network security and networks.