Comprehensive Survey on Enhanced approaches to Discover and Avert Greyhole attack in MANET

P. Padmapriya
Department of Computer Science and Engineering, Apollo Engineering College, Chennai, Tamilnadu, India
padmapriya044@gmail.com

Abstract —MANET, a Mobile Adhoc Network contains dynamic network of mobile nodes, a Self-configure and infrastructure less network. Generally, there is no centralized control over this network. Routing protocols plays a crucial role to communicate between the mobile nodes and share the required messages to each other. Because of adaptive nature, there may be a lot of security attacks & threats occurred in the network layer of MANET. It is a challenging task in-order to provide a secure communication between the mobile nodes from the various attackers .On account of frequent unpredictable topology changes in the network, it is difficult to maintain the route & also to discover the malicious nodes in Adhoc network. Attacks such as Black hole, Grey hole, and Wormhole which leads to a significant vulnerable threats concerned with network integrity and security for communicate between the nodes across the network in MANET. This paper presents an analysis of robust mechanisms on how to discover & mitigate the Greyhole attack from the network under the study of various categories of protocols & techniques to improve the security impacts & network efficiency.

Keywords— **MANET (Mobile Adhoc Network), Blackhole, Greyhole, Wormhole, Routing Protocols, Topology**

I. INTRODUCTION

Mobile Adhoc network which is flexible, self-organized mobile nodes with no centralized topology based network. Mobile nodes can be easily communicated with each other since there is no predefined infrastructure. Nodes in the network are dynamic, free and can also acts as a router. This makes this network for various applications such as Military battlefield purpose, disaster management, pollution monitoring, virtual conferences, etc. Two nodes can communicates directly in the network, only if they are within the radio transmission range. The nodes can also communicate via Multihop routing indirectly.

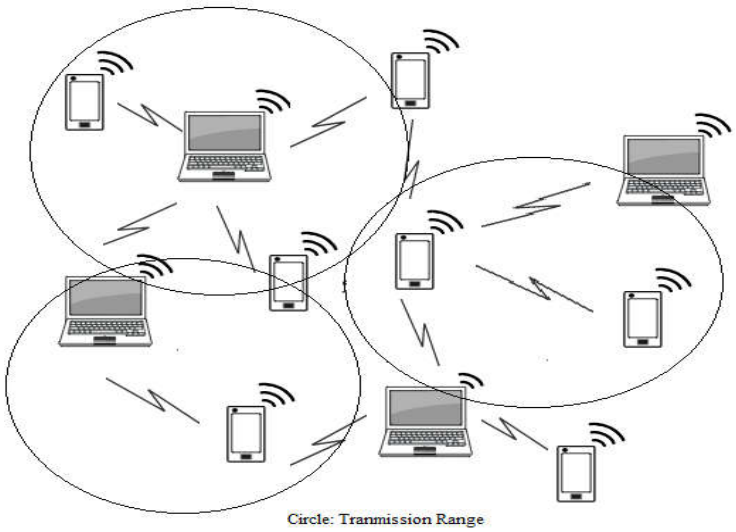

Fig. 2 Mobile Adhoc Network

To ensure the proper valid route traffic between the nodes across network, mobile adhoc network provide each device to continuously maintain the route information. MANET is more vulnerable than wired network due to dynamic nature of mobile nodes, scalability, limited security, resource availability and lack of centralized control. The routing depends on the trust and mutual collaboration among the mobile nodes. In adhoc network, trust is a major security concern, it can be easily compromised and it's a difficult task to identify the malicious nodes due to its dynamic and autonomous environment. Many issues concerned in MANET are Security, Confidentiality, Multicasting, Energy management, Routing methods, Node mobility and Scalability. Major challenging job in adhoc network is to provide robust security solutions under the various issues on mobile nodes across the network.

II. ROUTING PROTOCOL CATEGORIZATION AND ATTACKS IN MANET

A. Routing Protocol Categorization

Routing protocol plays a vital role for efficient transmission of packets among the nodes with secured route. Routing means a path to forward the packets from source node to destination nodes via intermediate nodes. Based on the routing protocols, the optimal routing path can be chosen under the various circumstances and to transmitting the packets to appropriate node with the help of various strategies implemented in it. Routing protocols can be categorized as 1) Table Driven protocol (Proactive), 2) Source initiated /on demand protocol (Reactive) and 3) Hybrid protocol.

1) Table driven / Proactive Routing Protocol:

Proactive Protocol is a table driven protocol where all the nodes information can be kept in the routing tables in advance and these information must be periodically updated when the network topology changes. Main advantages of this routing protocol are Lower Route Latency due to maintain routes at all the time & QOS guarantee. But, however there are various issues regarding to this protocol such as higher overhead due to frequently updating the route topology & High storage requirement. Various Protocols such as OLSR, DSDV are proactive in nature.

2) On Demand/Reactive Protocol:

In this, the routing information of the node can be established when it is needed (on demand).That is, When a node wants to send the packet to the other node, it initiates the route discovery process in order to get the route information on demand. Major features of using this protocol are Lower routing overhead, Low mobility and scalability if there is only low traffic. Larger route setup latency and flooding of path discovery packets are the major limitations of reactive protocol. AODV, DSR, TORA are some of the protocols for reactive routing.

3) Hybrid Protocol:

Hybrid protocol is a combination of proactive and reactive routing protocol to achieve improved security, network efficiency and scalability across the network in MANET. It combines the advantages of both reactive and proactive protocol for routing process. ZRP, ZHLS, CGSR are examples of this protocol type.

B. Attacks in MANET

A major challenge in MANET is security in which the data can be transmitted securely against the attackers. Various attacks arise from inside and outside the network. Attacks can cause the entire network routing communication to a total mess and disrupt the total performance of network. Attacks can be categorized on the basis of behavior as 1) Active attack 2) Passive attack.

1) Active attack: Nodes can changes or alter the messages or resources by gaining an authentication while communicating among the nodes in network. Examples of this attack include Black hole, DOS attack, Greyhole attack, repudiation etc.

2) Passive attack: This attack arises by listens the traffic over the network and it is difficult to find this attack since this attack doesn't modify the data packet while transmitting. It just only listen the traffic & gets the information which it needs. Examples include Snooping, Eavesdropping, and Traffic analysis.

Since there is no centralized control of nodes, the efficient routing protocol can be chosen to provide secured path for transmission against susceptible attackers and to detect and prevent attacks under the routing strategies. In the next section, the overview of Greyhole attack and the study about to discover and mitigate this attack is discussed.

III. AN OVERVIEW OF GREYHOLE ATTACK

A Greyhole attack is one of the active attacks which occur at a routing layer. In this attack, Greyhole is a node which is actively participating in the routing process to act as a normal node and abruptly switch out to a malicious node at any time and drops half of the packets without forwarding to the next hop/destination. This malicious node can selectively drops the packets instead of dropping all of the packets like Blackhole node. It can switch over to misbehaving state from normal state at any time. It is also known as selective forwarding attack.

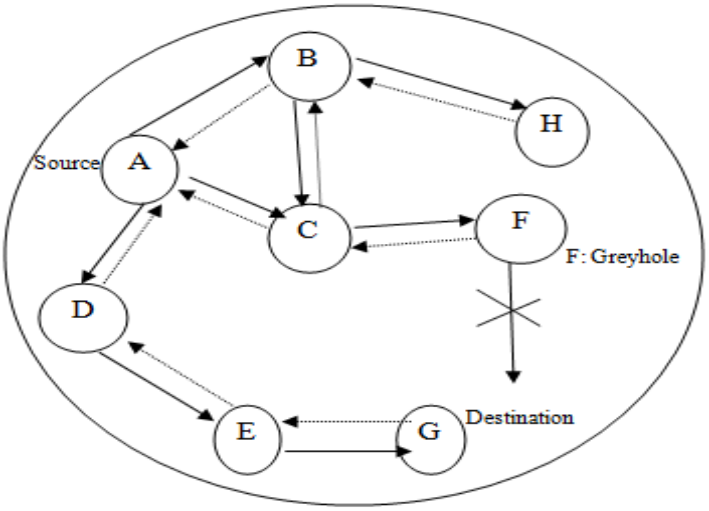

Fig. 2 Greyhole attack

Greyhole attack occurs on two phases. In Phase1, when the source node initiates the route discovery process the greyhole node can advertise itself as a shortest path to the source in the routing to reach the destination to forward the packets. This advertising takes place to interrupt the message on the route. In Phase2, the node acting as a genuine node can be transform to the mischievous node at any time to receive the packets and drop the packets on random basis or probability basis. So this attack can be unpredictable one while comparing with blackhole node since it can turns out between legitimate and malicious status. This attack occurs in the network leads to decrease the packet delivery ratio, throughput and degrade the performance of the overall network under various parameters. In this paper the different methodologies to be adopted to detect and avoid greyhole attack are discussed.

IV. METHODOLOGIES FOR DETECTION AND PREVENTION OF GREYHOLE ATTACK

Uzma Shaikh et al. "Intrusion detection & avoidance of black and greyhole node attacks using AODV protocol based MANET" proposed a method to detect greyhole attack by using intrusion detection system to provide more efficient mechanism for secure routing under AODV protocol. This method uses the sequence number ID of the mobile nodes to detect the malicious node. For every route reply and request of mobile nodes, the ID of target and ID of all mobile nodes in the network are to be listed in the request and reply routing table and this information keeps on watching by the base station node. When the AODV routing process initiates, the RREQ of mobile node checks if the ID of target mobile node is greater than or equal to ID of source node, then it is the malicious node (Greyhole), thereby the malicious node can be removed from RREQ table inorder to secure the routing path. Therefore, the greyhole node is identified and removed from the routing table for later transmissions and also the routing table is updated and broadcast in all other nearby nodes in the adhoc network to perform efficient communication. Performed simulation analysis and shown the packet delivery ratio can be improved with the help of IDS.

Ramireddy Kondaiah et al. "Trust and Fuzzy-Ant Colony Optimization based IDS for Secure Routing of MANET" used the fuzzy logic combined with Ant colony optimization to prevent the adhoc network. They proposed, using fuzzy process the levels of malicious nodes in network layers and the trust values of each node are calculated and updated regularly. With the help of swarm based ant colony technique, the trustworthy node to be chosen to ensure the secured route. Analyzed and showed the simulation results under TFACOIDS protocol in terms of Average packet delivery ratio (PDR), Throughput, overhead against various numbers of attackers involved in the network. By using this proposed combination of optimization technique, the data security can be enhanced under various attacks. It also shows that this algorithm is more efficient than other approaches to mitigate greyhole attack.

Luong thai NGOC et al. "Novel Algorithm based on Trust authentication Mechanisms to detect and Prevent Malicious node" analyzed and proposed the novel based approach to cover the Greyhole and prevent it by using Trust Authentication Mechanisms (TAM) under AODV protocol. Use the cryptographic RSA and Digital certificate(X509) standard techniques to authenticate the packets of the nodes. This proposed technique has shown ,in route discovery process involves 3 major steps:1)Digital Certificate to sign the valid node Packets 2) Finding Actual neighbors for authentication to check the Wormhole attack and finally 3)Packet Integrity authentication using Fake Keys to detect malicious nodes which uses the fake certificates for advertises as a legitimate node. Simulation can be done and conform that this trust based mechanism counter the attacks which is above 99% for all mobility scenarios. This paper also confirmed that the prevention of malicious nodes using fake key which is 100% prevention rate for all scenarios based on UDP packets transmission. However this technique has lower performance in terms of end to end delay and routing overhead.

Mohamed Abd-El-Azim et al. "IDS against blackhole & Greyhole attack for MANET" suggested a Fuzzy logic approach in order to detect the greyhole attack by Adaptive Neuro Fuzzy inference system and genetic algorithm. In this technique, initially get the fuzzy based parameters such as a Forward packet ratio (FPR) and average destination sequence Number can be calculated for each neighbor node and those data are one of the inputs of Fuzzy Inference System (FIS) to provide the Fidelity level of each node. In the optimization process of data preparations, the mapping can be carried out in which the malicious node maps to Low Fidelity level (0) and the normal node maps to High Fidelity Level (10) and in this stage involves training & testing.

Using genetic algorithm, the member function for each FIS to be calculated with the help of Mean square Error function and also the threshold value can b e derived from that process. If the node contains the value which is below the threshold (3) then the node is abnormal (which is malicious, Greyhole) and remove from routing table and also if it advertises as in a RREP in later transmission, this can be considered as a fake and source node sends an alert to all other nodes. This paper also performed the performance analysis of various mobility scenarios under the attack in terms of PDR and routing overhead. It also shown the PDR can be enhanced by using this proposed algorithm of FIS along with genetic algorithm. It shows the effectiveness of this algorithm by providing the secured route among the nodes.

"Detecting Greyhole & Blackhole attack using IDEA Cryptography in MANET", VenkataMounika Namburi et al. preferred a solution for the greyhole and blackhole attack detection with the help of International Data Encryption Algorithm (IDEA) which is a Symmetric Key Block cipher and combines with AODV protocol. This algorithm uses 56bit key to encrypt, decrypt and identify greyhole malicious node. In this approach, the source node gets the reply from both authorized and malicious node to advertise as shortest route and the malicious node get the data and drop it. Source node identify the malicious node by sending lot of RREQ messages to all other nodes including malicious node and get RREP again from that illegitimate node which it advertises as a shortest path to reach the destination. But the source node recognizes that node is a malicious and notifies to all other nodes in the network. This study proved that the efficient protection of transmitting the packets and the data against the unauthorized access by third parties (attackers).Energy level of all nodes played a vital role. It also showed the analysis of existing solution and proposed solution in Ns2 simulation in terms of throughput and energy level of nodes.

Nafei Zhu, Jingsha He et al. "An efficient Trust based scheme for secure and QOS routing in MANET"presented a trust based Quality of service mechanism to mitigate the attacks occurred in adhoc network. This methodology proposed to select the best forwarding node based on behavior in packet forwarding and QOS parameters such as Link quality, Channel quality and energy under AODV and adversary model protocol. From these QOS parameters, the trust value of each node can be derived in the routing process. Thereby for the trust update, using trust QOS routing strategy, Trust recommendation using Hello messages and Trust update methods, the secure path from source node to destination can be established against the attack. If the neighbor trust entry is less than the threshold, then it is a misbehavior node (greyhole) and updates to all other nodes. Performance comparison can be followed out and shown the PDR, residual energy consumption to be improved due to the enhanced QOS routing Scheme.

Niharika Gupta et al. "Prevent Greyhole attack in MANET Using Fuzzy logic" evince to preclude the greyhole node by using fuzzy logic rules and ABC (Artificial Bee Colony) algorithms to optimize the routing in adhoc network. In this paper, the greyhole can be detected under OLSR routing protocol with the help of ABC optimization. At first the node membership value compared with fuzzy rule membership for suspicion node at every time. That is, the membership value of the nodes which is greater than or equals the fuzzy membership value can be considered as a malicious node. Secondly, if there is a suspect occur checks the packet drop of that node and block it by ABC optimization. Thus, changes the route path between source node and target node can be made for the data packet transmission by invoking the fuzzy logic with OLSR and classify the grey hole node from the legitimate nodes across the network by ABC optimize objective function. Analysis shown that by evaluating parameters such as Bit error rate, Energy consumption & Packet Delivery Ratio, the Throughput rate is more than 90% improved, the PDR which increased by the rate of more than 94% when this optimization technique is employed under attack.

Rajwinder Kaur et al." Evaluate & Improve enhanced ZRP to detect and isolate greyhole attack in Adhoc network" have introduced to improve the Zone routing Protocol to counter and separate the greyhole node from the adhoc network. ZRP which is hybrid protocol combines the reactive and proactive benefits and this protocol is more efficient for larger network. By using this protocol, all the nodes can be formed as zones. All zones can be formed depends on the Zone radius. Nodes within the zone communicate via Intra zone routing protocol and the nodes can be communicated with the outside zone nodes through Inter zone routing protocol. In inter zone routing protocol, the Border gateway protocol (BGP) to be used for broadcast the request to the outside nodes of zone. By using this standard ZRP to identify the mischievous nodes is a difficult task. For this, they proposed an algorithm which is based on the fake route request packets from the nodes. By using Monitoring node on each zone, the malicious nodes can be identified by the fake route request packets. In this paper, the simulation can be performed under the enhanced ZRP protocol and the Standard ZRP protocol against the attack. Evaluate the parameters of delay, throughput and packet loss by using simulation graphs under the various protocol compared with enhanced ZRP to isolate greyhole node. This enhanced ZRP provide improved throughput rate. It also shown that the delay, Packet loss rate can be minimized by using this proposed approach.

Ruchi Tiwari et al. "Exposure and mitigation of Greyhole attack from AODV in MANET" suggested the isolation of greyhole attack under AODV protocol in adhoc network. This paper presented the periodic probabilistic rebroadcasting approach for secured transmission against the malicious node. It provides the solution based on the PDR in which the node total PDR is less than the threshold limit of 60, which is consider as a greyhole node and blocked it in RREQ. After perform the NS2 simulation and this concept shows that by using the unicasting process it saves the resources and presented this proposed solution is efficient through PDR, Routing Load and throughput compared with the existing solution.

"Detection & Prevention of greyhole attack using reputation system in MANET", Aishwarya Kundur et al. postulated how to identify and prevent the greyhole node in infrastructure less network. This paper exposed a MANET in a cluster like structure and the Node ID of each node can be assigned as Prime number in the network. Secure path can be selected based on Legitimacy value and Reputation level tables of every node by eliminating the illegitimate node with the help of CRCMD&R (Cluster and Reputation based Cooperative Malicious node Detection &Removal) strategy. This paper can show not only detects the single greyhole nodes, it also detects and isolates the cooperative greyhole nodes from the network. Performed the simulation analysis and provide the enhanced secure routing through data encryption have confirmed the effectiveness of this solution to trace the greyhole node.

V. CONCLUSION

MANET, which consists of autonomous moving mobile nodes, flexible nodes with decentralized network. Due to its changing nature, unpredictable topology, self-organizing characteristic and no predefined structure of network leads to a lot of security vulnerabilities occurred in the adhoc network. So, the major concern in MANET is security and to maintain the security across the network is very crucial and most challenging task. One of the major threats is Greyhole attack which is a severe threat in adhoc network and there is a need to identify and alleviate it from the other legitimate nodes to enhance the secure routing across the network. Thus, this paper proposed a survey of various methodologies to discover the greyhole attack in the network and also shown the approaches to mitigate the greyhole node from the routing process in MANET. Further research can be carried out to explore the new enhanced techniques to provide the more security by counter and avert this greyhole attack in Mobile adhoc network.

REFERENCES

[1] *Uzma Shaikh, Arokia Paul Rajan," Intrusion detection &avoidance of black and greyhole node attacks using AODV protocol based MANET", International Journal of Engineering & Technology, Vol 7, 2018.*

[2] *Ramireddy Kondaiah, Bachala Sathyanarayana, "Trust and Fuzzy-Ant Colony Optimization based Intrusion Detection System for Secure Routing of MANET" IJCSMC, Vol. 7, Issue. 4.*

[3] *Mohamed Abd-El-Azim, Hossam EL-Din Salah, and Menas Ebrahim," IDS against Black-Hole Attack for MANET", International Journal of Network Security, Vol.20, No.3, PP.585-592, May 2018.*

[4] *Muhammad Salman Pathan , Nafei Zhu, Jingsha He, Zulfiqar Ali Zardari, " An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs", MDPI, 2018.*

[5] *VenkataMounika Namburi,Sisir Bolisetty,Saketh Krishna Velugoti,T N Shankar," Detecting Greyhole & Blackhole attack using IDEA Cryptography in MANET", International Journal of Pure and Applied Mathematics, Volume 116 No. 5 ,2017.*

[6] *Luong Thai Ngoc, Vo Thanh Tu,"A Novel Algorithm based on Trust authentication Mechanisms to detect and Prevent Malicious node in Mobile Adhoc Network", Journal of Computer Science and Cybernetics, V.33, N.4 (2017).*

[7] *Ruchi Tiwari, Jyoti Jain, "Exposure and mitigation of Greyhole attack from AODV in MANET-An approach", International Journal of computer applications, Volume 165 – No.5, May 2017.*

[8] *Niharika Gupta, Pradeep Singh, " Prevention of Gray Hole Attack in MANET using Fuzzy Logic", (IJACMS), Volume 2, Issue 4, May, 2017.*

[9] *Qiang Liu, Jianping Yin,"FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs", IEEE Transactions on Wireless Communications.*

[10] *Diaa Eldein Mustafa Ahmed, Othman O. Khalifa, "A Comprehensive Classification of MANETs Routing Protocols", International Journal of Computer Applications Technology and Research Volume 6–Issue 3, 141-158, 2017, ISSN:-2319–8656.*

[11] *Aishwarya Kundur, Chaitali Parhate, Mrunali Chopade," Detection and Prevention of Gray hole Attack by Using Reputation System in MANET", International Journal of Innovative Research in Computer and Communication Engineering.*

[12] *Rajwinder Kaur,Vinay Bharadwaj, " To Evaluate and Improve ZRP Protocol to Detect and Isolate Gray Hole Attack in Mobile Ad-hoc Network", International Journal of computer applications, Volume 150 – No.12, September 2016.*

[13] *Nitesh A. Funde1, P. R. Pardhi, "Detection & Prevention Techniques to Black & Gray Hole Attacks in MANET: A Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013.*

[14] *Chamkaur Singh, Vikas Gupta, Gurmeet Kaur, "A Review Paper on Introduction to MANET", International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 1 - May 2014.*