RESEARCH ARTICLE OPEN ACCESS

A Review of Attacks, Routing Protocols and Security Scheme in MANET

Ms.Shaloopriya Jain [1], Ms Ruchika Mishra [2]
Department of Computer Science & Engineering
Adina Institute of Science & Technology
Sagar - India

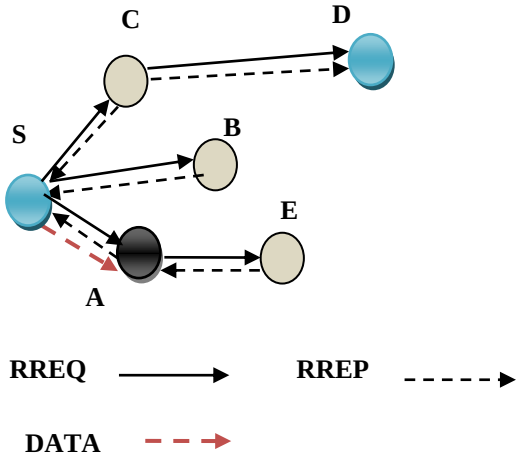
ABSTRACT
The proper communication in any network is the big problem that is occur due to the malicious functioning of attacker. The attackers only want to access the network at any cost and disturb the whole performance of network. Mobile ad hoc network (MANET) has emerged as a new edge of technology to provide anywhere, anytime communication. Due to its deployment nature, MANETs are more vulnerable to malicious attack. Due to the absence of centralized administration, security is the main issue in MANET and attackers are very easily modified the actual behavior and performance of network. The blackhole attack is packet dropping attack behaves like node at the time of connection establishment and after that forward false reply to sender and drop all the data packets. In this attack one or more malicious colluding nodes create a secure environment in the presence of other normal nodes in the network. Initially in this review we observe the performance of network from different security scheme and suppose to applied proper method to secure network against blackhole attack in MANET. The routing protocol is possible to defend the network from malicious activities. This survey is presents the overview of MANET, routing protocols, attacks and security scheme to secure network. In real life, such an altruistic attitude is more than often extremely difficult to realize and so we often find malicious nodes also present in the same network. Some of these are unknown nodes, which enter the network during its establishment or operation phase, perturb the network actual original activities.
Keywords: — Blackhole, MANET, Routing, Security, Review, Malicious nodes,

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) provides quick communication among nodes (like mobile or a laptop) to transfer the packets from one node to other. An example of an ad hoc network is given in figure 1 where nodes are communicating directly with each other. All the links between nodes are wireless. Bluetooth [1] is a typical example of such networks. These networks are independent of any fixed infrastructure or central entity like cellular networks [2] which requires fixed infrastructure to operate.

The nodes in MANET may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entail that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes. Due to this absence of authority, conventional techniques of network management and security are scarcely necessary for MANET. Any attacker or malicious node in the network can disturb the whole process or can even stop it. Several attacks like, blackhole, rushing etc [2] have been come into the picture under which a genuine node behaves in a malicious manner. It is quite difficult to define and detect such behavior of a node. Therefore, it becomes mandatory to define the normal and malicious behavior of a node. Whenever a node exhibit a malicious behavior in any attack, it assures the breach of security principles like availability, integrity, confidentiality etc [2]. An intruder takes advantage of the vulnerabilities (which is discussed in next section) presents in the ad hoc network and attacks the node which breaches the security principles.

In figure 1, sender node S wants to send data packets to a receiver node D in the network. Node A is a malicious node which is a Blackhole attacker node. The attacker replies false information about the route up to destination through highest sequence number. So that data packets sending by sender S towards A instead of D.



In a blackhole attack [2,3] an attacker receives packets from the sender and reply through false information of destination.,

and mentioned in figure 1. The attacker in network is exist in wireless transmission range of a single hop, it is simple or may be possible multiple and drop all the packets arrive with better metric than a normal multihop route. The blachhole attack is the routing attack and their behavior is also like as original blach hole means capture all the data packets. It is also possible for the attacker to forward each bit over the blackhole directly. Due to the nature of wireless transmission, the attacker can create a blackhole even for packets not addressed to itself by that all packets are forwarded through attacker and actual destination only wait for data. In world, such an unselfish angle is quite typically extraordinarily troublesome to appreciate and then we regularly notice malicious nodes conjointly contribution within the same network. A number of these are attacker nodes that affect the entire operation of network. The security scheme is necessary in network throughout its institution or operation, whereas others might originate indigenous by compromising an existing benevolent node. These malicious nodes will perform each Passive and Active attacks against the network state in next section.

II. ATTACK AND SECURITY ISSUE IN MANET

There are two kinds of attacks in MANET [4, 5] first is passive attack and another is active attack. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. .

A. Passive Attack

In passive attacks, an entrant the data changed while not sterilization it. The assailant doesn't actively initiate malicious actions to cheat different hosts. The goal of the assailant is to get data that's being transmitted, so violating the message confidentiality. Since the activity of the network isn't non-continuous, these attackers are tough to observe.

B. Active Attack:

In active attacks, an assailant actively participates in disrupting the conventional operation of the network services. A malicious host will produce a full of life attack by modifying packets or by introducing false data within the unintentional network. It confuses routing procedures and degrades network performance. Active attacks spirit into internal and external attacks.

C. External Attack

External Attacks are carried by nodes that aren't legitimate a part of the network. In external attacks, it's doable to disrupt the communication of a corporation from the automobile parking space ahead of the corporate workplace.

D. Internal Attack

Internal Attacks ar from compromised nodes that were once legitimates a part of the network. In unintentional wireless network as approved nodes, they're rather more severe and tough to observe compared to external attacks.

The most of the attackers [6] [7] ar moving the unintentional network performance and execute malicious activities at the time of causation and receiving the info. The attackers ar classified per totally different layer of network like Eavesdropping, jam assailant, blackhole attack, grayhole attack, byzantine attack [8], wormhole attack, DoS attack so on [6] [7], as a result of {the totally different|the various} assailant is clash the network performance at different layer.

Active attacks can be internal or external. Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a huge security concern for MANET.

E. Attacks using Modification

A node may attack by altering the protocol fields in messages or injecting routing messages with false values. To determine the shortest path, AODV uses the hop count parameter. A malicious node can locate the false hop counts. Also, it can set false value of route sequence numbers. This may cause redirection of network traffic. A DoS attack is launch by modifying source routes as well. DoS attack is easy to carry out but it is difficult to detect.

F. Attacks using Impersonation

By impersonating a node (spoofing), a malicious node can cause many attacks in MANET. For example, traffic that belongs to the impersonated node may be redirected to the malicious node. Loops may also be created by spoofing. The malicious node may take up identity of multiple nodes; it does not need to impersonate any node of the network.

G. Attacks using Fabrication

In fabrication attacks, false routing data is generated by an intruder. For example, false route error messages (RERR) and routing updates may disturb the network operations or consume node resources. Some well-known fabrication attacks is worm hole attack.

III. SECURITY ASPECT IN MANET

To make AODV secure, we need to understand security attributes and mechanisms. Security is applied with the mixture of processes, procedures, and systems which are used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation [5].

As MANETs use an open medium, all nodes can access data within the communication range. Therefore,

confidentiality should be obtained by preventing the unauthorized nodes to access data.

Authentication should be used to ensure the identity of source as well as neighbor nodes to prevent a node from accessing unauthorized resources and confidential information as well as to stop it from interfering operations of other nodes.

Integrity helps to prevent malicious nodes from altering data and resending it (called replay attack e.g. wormhole attack). Also, if a node sends a message, that node cannot deny that the message was sent by it which is called **non repudiation** [9].

To preserve against passive attacks conventional approaches like digital signature, encryption, authentication and access control (whether a node having appropriate access rights to access the network) should be considered. To defend against active attacks intrusion detection systems and cooperation enforcement mechanisms (reducing selfish behavior of a node) are useful. Encryption and authentication are based on asymmetric and symmetric cryptography [5]. To achieve data integrity and authentication, hash functions and digital signatures are really useful.

Secure Ad-hoc On Demand Distance Vector (SAODV) is an advanced version of AODV in which digital signature and has chains mechanisms are used. Each node uses digital signature for authentication and integrity in routing messages like RREQ, RREP and RRER. This signature is verified by neighbor nodes that receive the message. Hash chains are used to secure hop-count mechanism. Thus, SAODV addresses security of routing messages only; security of data exchange still remains unaddressed. Moreover, due to digital signatures, messages get bigger. Also, generating and verifying signatures add to the overhead, especially when double signatures mechanism is used.

IV. NEED OF SECURITY IN AD HOC NETWORK

Though the mobile ad-hoc networks square measure wide used however still it's some weakness in it. Consequently, convenient may be would like of security to defend such issues. An intruder utilizes this weakness to grasp concerning the network processes so attack the network. Following square measure some contribution vulnerability in impromptu networks.

A. Mobility

Every node in mobile ad-hoc network is movable. It will be part of or leave a network at any instant of your time while not informing any node. This provides probability to interloper to simply enter within the network and even collaborating in its operations.

B. Open Wireless Medium

All the communication between nodes is happening through the medium of air rather than wires. An interloper will simply access this medium to achieve data concerning the communication or will simply entice it.

C. Resource Constraint

Each node in mobile impromptu network has restricted resources like battery, machine power, information measure etc. an interloper will while not cause waste these restricted resources so as to form it untouchable to perform.

D. Dynamic Network Topology

Because the nodes square measure extremely movable in nature, therefore the topology changes anytime the communication takes place. The packets from supply to destination might take completely different path for announcement. An interloper will initiate itself in any path.

E. Scalability

Mobile Ad-hoc network might contain variety of nodes. This variety isn't fastened. In a very network of its vary, as several as variety of nodes will participate. Intruder merely takes advantage of this parameter as there's no limitation on variety of nodes.

F. Reliability

All the wireless communication is proscribed to an vary a variety a spread of one hundred meter that puts a constraint on nodes to be in range for establishing communication. as a result of this restricted vary, some knowledge errors also are generated. For assaultive a specific node, an intruder has to be in it's vary.

V. PREVIOUS WORK IN FIELD OF ATTACK

The previous work in field of blackhole is mentioned in this section. These work are also efficient and provides information about the work is already done in field of attack.

In [10] Sathish M et.al proposed security scheme to protect the network from black hole attacks, it is important to discover malicious nodes during the route discovery process, when they pass fabricated RREP imitating the source node. Our proposed methodology does precisely the same. Based on next hop information and destination sequence number that can be extracted from RREPs, this scheme handles single and collaborative black hole attacks with extenuated computational, routing and storage overhead.

In this work [11] V. Keerthika et.al proposed Direct/indirect trust is computed using normalized Route Reply misbehavior factor, link quality, and successful deliveries to mitigate black hole attack. The hypothesis that node capability is also essential for efficient functioning of the network is not considered. In this work it is proposed to include network parameters to compute trust. Nodes travel a long distance in space among one in MANETs and are not specific of another's reliability because of not gathering sufficient evidence. The model is needed to represent uncertainty accordingly with common uncertainty. Direct/indirect trust is computed to track a node's trustworthiness in this work.

In this paper [12] Raquel Lacuesta et.al can establish a secure self-configured environment for data distribution and resources and services sharing among users. A user is able to join the network because he/she knows someone that belongs to it. Thus, the certification authority is distributed between the users that trust the new user. The network management is also distributed, which allows the network to have a distributed name service. We apply asymmetric cryptography, where each device has a public-private key pair for device identification

and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification. Spontaneous ad hoc networks require well defined, efficient, and user-friendly security mechanisms. Tasks to be performed include: user

identification, their authorization, address assignment, name service, operation, and safety.

In [13] Raj et al. proposed DPRAODV an additional check is done to find whether the RREP se<L no value is higher than the threshold value as compared to normal AODV. If the RREP se<L no value ishigher than the threshold value, the node is considered to be malicious and that node is added to the black list. As the node detects a malicious node, it sends an ALARM packet to its neighbors. This ALARM packet has black listed node as a parameter. Later, if any other node receives the RREP packet it checks the black list. If that node is black listed, it simply ignores it and does not receive reply from that node again. The simulation result shows that the packet delivery ratio is improved as compared to AODV.

In [14] D. B. Johnson et al proposed scheme in which source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination. The source node waits for RREP packet to arrive from more than two nodes. In ad hoc networks, the redundant paths in most of the time have some shared hops or nodes. When source node receives RREPs, if routes to destination shared hops, source node can recognize the safe route to destination. But, this method can cause the routing delay. Since a node has to wait for RREP packet to arrive from more than two nodes. Therefore, a method that can prevent the attack without increasing the routing overhead and the routing delay is required.

In [15] Puttini R et. al. proposed a mobile agent based IDS system in which mobile agents are transferred to wireless nodes and perform IDS operations to detect the intrusions. The work done in this paper is oriented on MIB and focused more on functionality and feasibility validation or the design. They have focused only on working of IDS in distributed systems and also another future important issue is the security of the mobile agent platform.

In [16] D. Barman et al. proposed a new Intrusion Detection System (IDS) based on Mobile Agents. The approach uses a set of Mobile Agent (MA) that can move from one node to another node within a network. This as a whole reduces network bandwidth consumption by moving the computation for data analysis to the location of the intrusion. Besides, it has been established that the proposed method also decreases the computation overhead in each node in the network.

In [17] Panthi N.K et. al. had proposed a scheme which not only confirms the security of data but also guarantees the uninterrupted operation of agent by utilizing a dummy agent and composite acknowledgement technique. Their simulation also shows that no agent blocked for any number of faulty nodes. Some draw back shows the increase in delay, they have not considered the security of monitoring agent, the processing time needed is also higher. They surveyed three approaches for the problem of mobile agent protection. The three approaches are chosen because each approach is very uniquely implemented and has strengths that other approaches do not have; they choose Partial result authentication code approach because it can protect results from mobile agents. Computing with encrypted functions approaches is chosen because it tries to scramble code and data together. An obfuscated code approach is chosen because it scrambles an agent's code in such a way that no one is able to gain a complete understanding of its function .

In [18], L.Tamilselvan et al., proposes the notion of 'Fidelity Table. Here, every participating node is allotted a particular fidelity level, a measure of reliability. Whenever a source node broadcasts a RREQ and holds up, the incoming RREPs are gathered in its Response Table. If the average of the fidelity level of RREP sending node (RREPN) and its next hop node (NHN) in the route is found to be over a predetermined threshold, the RREPN is considered as trustworthy. Therefore, on the receipt of multiple RREPs, the one with the highest fidelity level is selected. However, if multiple nodes have the same fidelity level, the RREP with the minimal hop count is chosen. Finally, routing is accomplished via the selected path.

In [19] Sun B proposed scheme based on the neighbor set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are: first step collect neighbor set information. Second step determine whether there exists a black hole attack. In Response procedure, Source node sends a Modify Route Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (1M) from source to destination. This scheme effectively and efficiently detects black hole attack without introducing much routing control overhead to the network.

VI. CONCLUSION

The dynamic network called MANET is very popular for short range communication between the mobile devices. This research is very useful in field of security to evaluate the network performance in case of attack and proposed previous security scheme. At present network, security is one of the challenging tasks in central administration based network now on in MANET i.e no admin in network security is major concern. The attack in MANET is easily loss the data and degrades the network routing performance. In this review paper we focus on many types of attack but specially highlight on the blackhole attack in MANET. The previous work is provides the idea about how the different security scheme is apply the proper procedure to secure MANET routing performance.

VII. EXPECTED OUTCOME

In this review paper, an exhaustive simulation for MANET will do by using AODV routing protocols and the effect of the

presence of single blackhole and multiple blackhole attack will simulated. Significant performance parameters such as infection rate throughput, delay in different node density is measured. The study focuses on how performance of network will affected under blackhole attack in a network. The study here establishes the foundation for future work towards designing a mechanism to identify the nodes, which are actively involved in the blackhole attack. We made our simulations using ns-2 (network simulator version 2.31). Having implemented a new routing protocol which simulates the black hole behavior in ns-2, we performed tests on different topologies to compare the network performance with and Security on blackholes in the network.

REFERENCES

[1] C.Siva Ram Murthy and B S Manoj, 'Mobile Ad Hoc Networks-Architecture and Protocols", Pearson Education, ISBN 81-317-0688-5 ,2004.

[2] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols, Springer, 2005.

[3] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, April. 2004.

[4] Monis Akhlaq, M. Noman Jafri, Muzammil A. Khan and Barber Aslam,"Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology 16, pp. 29-33, 2006.

[5] Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", European Journal of Scientific Research, pp. 430-443, 2009.

[6] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, " A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, 2010.

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,"Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 1-38, @ 2006 Springer.

[8] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[9] Khin Sandar Win," Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 48, pp. 422-428, 2008.

[10] Sathish, Arumugam, S.Neelavathy Pari, Harikrishnan V," Detection of Single and Collaborative Black Hole Attack in MANET", This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.

[11] V. Keerthika, N. Malarvizhi, "Migrating Blackhole Attack using Trust with AODV in MANET, IEEE, 2016

[12] Raquel Lacuesta, Jaime Lloret, Miguel Garcia and Lourdes Penalver "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4, 629-641, April 2013.

[13] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANEr', International Journal of Computer Science Issue, Vol. 2, pp 54-59, 2009.

[14] D. B. Johnson, D.A. Maltz, and J. Broch, DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", Ad Hoc Networking, pp. 139-172, 2001.

[15] Puttini R. and jean-Mare Percher-"A Fully Distributed IDS for MANET",IEEE Int.Conference ,2004.

[16] D. Barman Roy1 and R. Chaki" MADSN: Mobile Agent Based Detection of Selfish Node in MANET" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011.

[17] Panthi N.K. et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, "Securing Mobile Agent Using Dummy and Monitoring Mobile Agents" Vol. 1 (4) , pp. 208-211, 2010.

[18] L.Tamilselvan, Dr.V. Sankaranarayanan, "Prevention of Co-operativeBblack hole attack in MANET ", Journal of Networks,, 2008,pp. 13– 20.

[19] Sun B, Guan Y, Chen J, Pooch UW , " Detecting Black-hole Attack in Mobile Ad Hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[20] Karuturi Satish, K. Ramesh et al., "Intrusion Determent using Dempster-Shafer Theory in MANET Routing", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 1, pp. 37-41, 2015.