Distinctiveness of Manet and its Security Issues: A Review

P. Tamilselvi[1], C. Ganeshbabu[2] and V. Arthi[3]
[1]Asst. Professor, Sri Eshwar College of Engineering/ECE Department, Coimbatore, India
Email: ttamil_p@yahoo.com
[2]Professor, Bannari Amman Institute of Technology/ECE Department, Sathyamangalam, India
Email: bits_babu@yahoo.co.in
[3] Assoc. Professor, CVR College of Engineering/ECE Department, Hyderabad, India
Email: arthi.psv@gmail.com

Abstract: **Manet is a wireless network that has a group of nodes that can move in any direction. Manets do not have a particular infrastructure. So, they are not controlled by a central system. The autonomous nodes have arbitrary movement inside the network which can create momentary dynamic network. Because of this, the topology of the network often changes. Manets are nowadays used for commercial purposes due to their distinguishing properties. But these networks have to face a lot of security related issues. Also Manet has restricted bandwidth, dynamic topology and has to share the wireless medium. Because of the usage of shared medium, security challenges has become a primary concern to provide secure communication. The aim of the paper is to provide a complete knowledge about the various routing protocols used, characteristics of Manet and security issues the network has. To achieve our aim, literature survey is done and the related information is collected. In order to provide a secure communication in manet, attacks should be recognized and prevented.**

Index Terms**: Black hole, Routing protocol, Manet, Security attack**

I. INTRODUCTION

A mobile adhoc network is a group of mobile nodes that do not have an access point or any infrastructure for proper opertion. Ad hoc networks are to be used in tactical networks for Military communication and operations, Automated battlefields. In sensor networks to automate everyday functions like earth and weather activities. Manets are also used in emergency situations like earthquakes, disaster recovery and commando operations. One of the main security threats is that nodes may become malicious. Black hole and Gray hole attacks are major types of malicious attacks.

A. Black hole attack

A Black hole attack is an active attack where the nodes captures all the data packets and drop them, Black hole attack is depicted in Fig.1. In this attack the malicious node broadcasts to all its neighboring nodes that it has shortest route to destination without checking the routing table. Receiving this information, the source node will transmit its data packet to the malicious node. The malicious node will receive the data packets and drop all the data without forwarding them to destination. This is the black hole attack in MANETs.

B. Gray hole attack

A Gray hole attack is an extension of black hole attack. Attackers drop data packets from selected nodes while forwarding the data from other nodes. The behavior of malicious nodes is unpredictable. The attack cannot be easily detected. The Gray hole may behave maliciously for some time and return to normal behavior later.

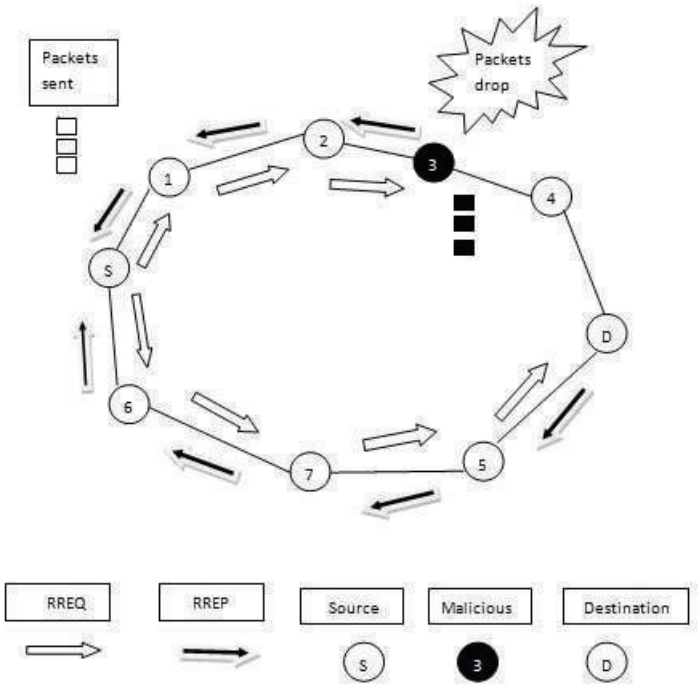

Figure1. Manet with black hole

II. CHARACTERISTICS

2.1. Multi-hop transmission

Multi-hop transmission is applied to transmit messages when the source and destination are not closer and they are apart. So, the MANETs use multi-hop transmission when the network size is large and one-hop transmission is not possible. One or more intermediate nodes are used to forward the message packets when the source and destination are not directly connected.

 doi:10.32377/cvrjst1402

2.2. Distributed nature of operation

There is no centralized control system to monitor and control the functions of the network. So the nodes present in the network takes the responsibility and collaborates to implement the functions such as routing and security.

2.3. Self directed

In MANET, the role of host and router are done by the same mobile node. It means that a node has ability to work both as host and router. Nodes perform switching functions as router and so endpoints and switches are same.

2.4. Dynamically varying topology

The topology of the Manets is dynamic as the nodes in the network are mobile. As time goes on, nodes move in random manner and so routes are established dynamically.

2.5. Poor link capacity

Compared to wired links, the reliability, scalability, efficiency and capacity of wireless links are often less. The communication channel is subject to noise, fading, interference and has less bandwidth than a wired network.

2.6. Absence of Infrastructure

Nodes in ad-hoc networks are able to operate independently without any fixed infrastructure.

III. ROUTING PROTOCOLS

Routing protocols are a set of rules used for connecting a source and destination for transmission of message packets in a network. There are different types of routing protocols used in MANETs. The appropriate routing protocols are chosen according to the network circumstances and requirements. The routing protocol's classification are:

3.1. Proactive Routing Protocols

The other name of Proactive routing protocols is table-driven routing protocols. The contents present in the routing table are used for routing. In this protocol, each node maintains a routing table that stores all the updates related to the changes in the structure of the network. Data renewal is done every time network structure changes. Proactive protocols are not suitable for large networks because for each node, entries should be made in the routing table which is complex. DSDV, OLSR, WRP etc are some of the proactive routing protocols.

3.2. Reactive Routing Protocols

In reactive routing protocol, whenever necessary the routes are discovered. So this protocol is called on demand routing protocol. Whenever there is a need for new route, route discovery is initiated by the nodes. Nodes with appropriate routes reply to the source. DSR, AODV, TORA and LMR are some of the reactive routing protocols. There are two mechanisms in this protocol:

3.2.1. Route discovery

In this phase source node initiates route discovery on demand basis. Source node checks its route cache for the available route from source to destination. If the required route is not available, the route discovery is initiated. The source generates a request message. The request message contains the address of the intermediate nodes in the path and the destination node.

3.2.2. Route maintenance

The happenings like link breakage cause route failure whenever the topology of the network changes. Acknowledgement mechanism is used in reactive protocols for checking the reliability and to maintain the routes.

3.3. Hybrid Routing Protocol

Both proactive and reactive protocols have some advantages and disadvantages. Hybrid protocol combines the advantage of both proactive and reactive protocols. The overhead is high in proactive routing protocols compared to reactive routing protocols. The latency is less in proactive routing protocols compared to reactive routing protocols. Hybrid protocol is appropriate for large networks where lots of nodes are present. Both the 'on- demand technique' and 'routing- table maintenance' are used in hybrid routing protocol. It avoids latency and overhead problems in the network. In large networks, the network is divided into a set of zones. Proactive approach is used for routing inside the zone. Reactive approach for routing outside the zone routing. MANET like ZRP, SHRP etc is some of the types of hybrid routing protocol.

IV. CHALLENGES

The MANET has to face several challenges that must be analyzed.

4.1. Routing

Routing the packets between any pair of nodes is not easy as the topology of the network changes. The protocols chosen may be reactive routing or proactive routing. The nodes have a random motion in the network and so multicast routing is another challenge. Routes between the nodes may have single hop or multiple hops. Multi hop communication is more complex than the single hop communication.

4.2. Quality of Service

The environment for Manet is constantly changing and so achieving necessary quality of service levels will be a challenge. Appropriate routing methods are selected so as to provide good quality of service.

4.3 Security and Reliability

Ad hoc networks are not secure always. Various schemes of authentication should be applied to provide secure communication. Some nodes may not be reliable and may cause hazards to the adhoc network. So, checking the node's reliability is very important.

4.4. Power Consumption

For most of the light-weight mobile devices, the power consumption is an important factor to be considered. Power conservation and power-aware routing must be used for optimal functioning of the network.

V. SECURITY

The following are some security criteria and attacks that occur in Manet:

5.1. Security Criteria

5.1.1. Availability

The term Availability means that all the assigned services should be provided by the node in any condition. This security criterion is violated mainly during the denial-of-service attacks. In the denial-of-service attack, the selfish nodes deny some of the network services.

5.1.2. Authentication

This guarantees that all the nodes participating in communication are genuine and not impersonators. It is necessary that all communication entities should prove their identities. The attacker could act as a beginning node if authentication mechanism is not used in the network. The attacker can thus get rights to see the confidential information. The attacker can also insert some bogus messages and collapse the normal network operations.

5.1.3. Confidentiality

Information is confidential only if the authorized members can get the access. All other entities which does not have authorization, cannot use the confidential data. All the data in the network should be kept confidential.

5.1.4. Non-repudiation

The sender and the receiver of a message cannot refuse the transmission or reception of message. Non-repudiation is used when there is a need to differentiate a node with some abnormal behavior. A node can notify an abnormal behavior node with the evidence of the erroneous message received

5.1.5. Integrity

Message being transmitted should be real. Integrity is spoiled by two ways. One is malicious altering and the other is accidental altering. In malicious altering, the message is changed or dropped repeatedly by an attacker. In accidental altering, link failure in the network may lead alteration in the message or sometimes loss of message.

5.1.6 *Attacks using Fabrication*

False routing messages are generated and transmitted to the nodes which require routes. Such types of attacks are difficult to detect.

5.2. Attacks on Manet

5.2.1. Location Disclosure

Location disclosure is an attack where a compromise is done in the private information of an ad hoc network. An analysis is done on the traffic generated by the network in order to find a node's location and also the network's structure.

5.2.2. Black Hole

In a black hole attack, whenever the source sends route requests, a malicious node gives false route replies to the route requests. Black hole node declares that it is having the shortest path to a destination. Believing these false route replies, the source transmits data packets to the malicious node. The malicious node captures the data packets and drops them instead of transmitting them to destination.

5.2.3. Replay

Another attack that heavily attacks the performance of MANET is replay attack. The valid signed messages are captured and retransmitted by the replay attacker. The transmitter and the receiver nodes use timestamp for validating the signed messages. The freshness of routes is affected by this attack.

5.2.4. Wormhole

The wormhole attack is one of the possible severe attacks. In this attack, two malicious nodes that are involved in the network cooperate to execute this attack. Wormhole nodes fake a route that is shorter than the original route, Wormhole node can easily attack the network without knowing about the network. The two attackers take the control of the wormhole link between the two nodes.

5.2.5. Denial of Service

The routing operation and also the entire operation of the network is affected by the denial of service attack. The resources of the communicating nodes are consumed by the routing table overflow attack. The malicious node floods the network with fake route creation and stops the creation of legal routes.

5.2.6. Masquerading

During the neighbor acquisition process, an outside intruder compromises the authentication system and joins to the existing communication link and masquerades an IS. The danger of masquerading is the same as that of a compromised IS.

5.2.7. Impersonation

The attacker creates a fake belief that it is a friend of the genuine node if there is no authentication mechanism prevailing in the network. The malicious nodes can then join the network as the normal nodes. The malicious nodes start their attack by propagating fake routing information and gets inappropriate access to the confidential information.

5.2.8. Eavesdropping

Eavesdropping attack obtains the confidential information from the nodes that should not be shared to any others during the communication. The information is made confidential by use of various keys like public key, private key, location and passwords of the nodes. The unauthorized nodes cannot get access to the confidential information.

VI. RELATED WORK

In [3], author focuses on grey hole attack. Grey hole attack affects the routing services provided by the network. Adhoc-on-demand (AODV) protocol is used for routing of data packets. This paper discusses the security issues and also the layered architecture of Manet. This paper also gives

the various applications of Manet. It also briefs the various work done in the area of adhoc network.

In [5], author proposes real time monitoring system AODV (RTMAODV). Real time monitoring method is used by the neighbor node to detect and prevent grey hole. Source sends Route request RREQ. On receiving RREQ, some nodes reply to those RREQs. These nodes are monitored in promiscuous mode. This is done by neighbors of the nodes who send RREP to detect the malicious behavior.

In [6], author proposes Trust Based Secure On Demand Routing protocol called "TSDRP". This proposed routing protocol can use for increased size of network. TSDRP protocol transmits data packets to the destination nodes even in the presence of malicious node. Performance analysis is done by comparing the proposed TSDRP and AODV protocol by measuring various parameters.

In [8], author put forward a scheme "BLACK HOLE AODV". Implementing this protocol, black hole is identified and its effect is nullified. This paper also gives the consequences of black hole attack. The performance of the network with and without black hole is analyzed.

In [9], author uses a second-best route for the destination to find the malicious behavior. Source broadcasts route request RREQ to get the route to destination. When the route reply RREP is received by the source, it transmits the confirmation packet using the second-best route to the destination. Source confirms that the destination has a route to the node which generates the RREP or to the Next_Hop_Node of the node that generates RREP. If the destination has no route to these nodes, both the node which creates RREP and its Next_Hop_Node will be assumed to be malicious nodes. The source node can detect cooperative malicious nodes by using this scheme. But in the case of more than two cooperative malicious nodes, this approach is not useful.

In [10], author proposed a scheme which identifies the malicious nodes by using aggregate signature algorithm. It associates three algorithms.
(1) The proof creating algorithm: Whenever the nodes involved in a communication receive a message, they create a proof that is based on aggregate signature algorithm.
(2) The checkup algorithm: This algorithm is called when the source node suspects that the transmitted packets are dropped. If the destination reports that it does not receive all transmitted packets, it will invoke this algorithm to detect the malicious node.
(3) The diagnosis algorithm works with the results of check up algorithm. Simulation is done in ns2 simulator. Using this proposed method, overhead is reduced and packet delivery ratio is improved.

In [11], AODV routing protocol is used to reduce the effect of gray hole attack. The proposed method first set the waiting time for the source node to receive the RREQ coming from other nodes. This waiting time is then added to the current time. RR-table stores the replies with high destination sequence number as the first entry in the table. Then the first destination sequence number is compared with the source node sequence number. The entry in the RR-table is removed when the differences between them are high. The next node id that has the higher destination sequence number is selected. The content of RR-table is sorted according to the DSEQ-NO column.

In [13], authors proposed an intrusion detection system named Enhanced Adaptive Acknowledge (EAACK) . Two encryption techniques DSA and RSA are used in EAACK and their performances are compared in MANET. DSA scheme generates less overhead than RSA. EAACK prevent attackers from initiating forged acknowledgment attack

In [15], author proposes Black hole Avoidance Protocol for wireless network (BAAP). Adhoc on demand multipath distance vector (AOMDV) is used in this proposed method. Each and every mode in this protocol makes cooperation with their neighbor nodes to form the reliable path to destination node. Performance metrics are measured which shows that packet loss is less than AODV. Packet Loss increases as mobility increases. In route discovery process, an intermediate node will try to create a route and this route should not contain a node whose legitimacy ratio is lesser than the lower threshold level.

In [18], author proposed a black hole avoidance scheme. An enhancement is made in the AODV routing protocol to eliminate the black hole. The source first sends the route request and waits for responses from all neighboring nodes with which it gets a reliable route. According to this proposed scheme the source node should not send data packets immediately after receiving the first reply.
"Timer Expired Table" is used to set timer after the reception of first reply. This table stores the sequence number of the packet. "Collect Route Reply Table" is used to store arrival time. Node's waiting time depends on the distance. Entries in the table help to identify malicious node.

In [19], author presented a black hole detection scheme. In this method, when the source node receives RREP packets, it generates a new RREQ. RREQ has the highest sequence number and it is unicast through the route in which the RREP packet was received. Malicious node generates a RREP with highest sequence number on receiving RREQ. Malicious node sends the fake RREP packet to the source node. Now source identifies the malicious node. This method has very less overhead.

In [20], author analyses all the security issues in the mobile ad hoc networks, which is a great hindrance to the working of Manet. Intrusion detection techniques and cluster based intrusion detection techniques are clearly explained. Misbehavior detection through cross layer analyses is also briefed.

In [21], author gives a thorough study on detection of misbehavior links and malicious nodes. The routing protocols used by Manets are also explained. The paper also tells how to protect the connection between the mobile

nodes in a multi hop network. The security issues are analyzed and the state-of-the-art security proposals that protect the MANET link are detailed.

In [22], author gives a brief introduction on Manets. A review is done on the previous research work done on the Manet to provide a complete security solution for efficient communication.

VII. Conclusions

Characteristics of Manet, challenges faced and the various security issues are discussed in this paper. Because of uncertainty in the wireless environment, Mobile adhoc networks needs protection from the vulnerabilities caused by attackers. This paper put forward the research works done in the Manets to provide security. All the research works aims at providing better quality of service in the adverse environment nullifying the attack of intruders.

References

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang,Han-Chieh, Chao and Chin-Feng, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in IEEE Systems Journal VOL 9. NO.1.Marrch 2015,pp.65-75

[2] Hitender Gupta and Harsh Aggarwal,"Simulation to detect and removal of black hole in Manet", SSRG Intenational Journal of Electronics and Communication Engineering, April 2015,pp.35-39

[3] Rakesh Ranjan, Nirnemesh Kumar Singh, Ajay Singh, Security Issues of Grey Hole Attacks in MANET" nternational Conference on Computing, Communication nd Automation (ICCCA 2015).

[4] Tao Shu and Marwan Krunz," Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireles Ad Hoc Networks", IEEE Transactions On Mobile Computing, Vol 14,No.4,April 2015, Pp.813-828.

[5] Anishi Gupta, "Mitigation Algorithm against Grey Hole Attack Using Real Time Monitoring for AODV Routing Protocol in MANET" IEEE 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom).

[6] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[7] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th Int'l. Conference Mobile Comp. Net., pp. 255-265, August 2000.

[8] Semih Dokurer, Y.M.Erten and Can Erkin Acar, "Performance analysis of ad-hoc networks under black hole attacks" IEEE conference Procedings,March 2007.

[9] N-W. Lo and F.-L. Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET," in Intelligent Technologies and Engineering Systems. vol. 234, ed: Springer New York,2013, pp. 59-65.

[10] G. Xiaopeng and C. Wei "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" IFIP International Conference on Network and Parallel Computing, 2007.

[11] Mr.ChetanS.Dhamande and H.R.Deshmukh, "A Efficient way To Minimize the Impact of Gray Hole Attack in AdhocNetwork ", International Journal of Emerging Technology and Advanced Engineering, Volume 2, February 2012.

[12] P. Agrawal, R. K. Ghosh, and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks," in Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication 310–314.

[13] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions On Industrial Electronics, Vol. 60, No. 3, March 2013.

[14] Y. Zhang, W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," 6th Int'l. Conference Mobile Comp. Net., Mobicom 2000, pp. 275-283, August 2000.

[15] Saurabh Gupta, Subrat Kar, S.Dharmaraj, "BAAP:Black hole Attack Avoidence Protocol For Wireless Network",International Conference on Computer and Communication Technology (ICCCT)-2011.

[16] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting blackhole attack on aodv-based mobile ad hoc networks by dynamic learning method," International conference on wireless networks vol. 5, no. 3, pp. 338–346, Nov. 2007.

[17] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative black hole attack in wireless ad hoc networks," in International Conference (ICWN'03), Las Vegas, Nevada, USA, 2003.

[18] LathaTamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), IEEE

[19] S. Banerjee, M. Sardar, and K. Majumder, "AODV Based Black-Hole Attack Mitigation in MANET," in Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013. vol. 247,

[20] Pradeep Rai and Shubha Singh, "A Review of 'MANET's Security Aspects and Challenges" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[21] Rashmi Mahajan and S. M. Patil, "A Review of 'MANET's Security Aspect and Challenges with Comprehensive Study of SIDS for Discovering Malicious Nodes" International Journal of Innovative Science,Engineering & Technology, Vol. 1 Issue 6 August 2014.

[22] Komal Khedkar and Shubham Josh, "A Review on Secure Routing Protocols in MANET", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 11, November 2014.