International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-3, Issue-7, July 2015

An Introduction to MANETS

Ritika Sharma, Bhawna Singla

***Abstract*— The wireless mobile Ad-hoc network (MANET) is a collection of wireless mobile nodes that can be formed without the need of any pre-existing infrastructure. MANET is an autonomous system in which each node enters and leaves the network at any point of time. The features like wireless medium, randomly changing topology, dispersed alliance makes MANETs more exposed to a variety of security attacks such as worm hole, black hole, flooding attack etc. In this paper we study mobile ad-hoc network and its characteristics, advantages and disadvantages, routing protocols and its classification of security attacks.**

***Index Terms*— Mobile Ad-hoc Network (MANET), Routing Protocols, Black Hole Attack, Ad hoc On-demand Multipath Distance Vector (AOMDV)**

I. INTRODUCTION

Mobile Ad-hoc Network is a group of the mobile nodes that is created without the help of any existing network infrastructure. The MANET is self configurable network where nodes connect as well as disconnect from the other nodes in the network involuntarily at any point of time. The characteristics of the MANETs are node to node connection, flexibility, dispersed operation, addressing mobility, etc. Routing of the data in the MANETs are made on the basis of the node discovery i.e. the node accept the data and forwards it to adjacent node in the path for the further transmission in order that it reaches to a particular destination. Each node works like a relay agent to route the data traffic. of MANET is available to all the users because of its dynamic nature. The user may be a legitimate user or the malicious node which replicate the data or attack the network.

Fig.1 shows an ad-hoc network with three nodes. Node 1 and Node 3 are out of the range of each other. However Node 2 is used to forward packets between Node 1and Node 2. The Node 2 acts as a router and these three nodes collectively form an ad-hoc network.

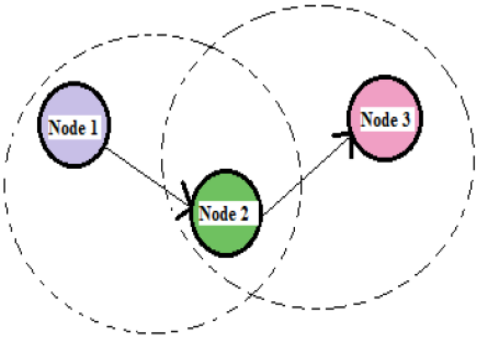

Fig. 1 Example of mobile ad-hoc network

Ritika Sharma, Computer Science and Engineering, N.C. College of Engineering, Israna, Panipat, India
Bhawna Singla, Computer Science and Engineering, N.C. College of Engineering, Israna,Panipat, India

II. CHARACTERISTICS OF MANET

Autonomous System: Each node in a MANET is an independent node. The nodes in the network work both as a host and as a router.

Dynamic topologies: In the mobile ad hoc network since the nodes move randomly, the multi hop network topology unpredictably changes, resulting in route changes, probably packet losses and several network partitions.

Multi hop routing: When one node transmits information to some other node which is not in its communication range, the packet is sent forward by means of one or more intermediate nodes.

III. ADVANTAGES AND DISADVANTAGES OF MANET

The Advantages of MANET are as follows :

- The networks can be formed at any place and time.
- The network is independent from central network administration. Due to self-configuring network, nodes act as routers. These networks are less costly as compared to wired network.
- Access to information is available regardless of their geographical position.
- Because of decentralized supervision they are robust.
- Enhanced flexibility.

The following are the disadvantages of MANET:

Non Secure Boundaries:

MANET is exposed to different variety of attacks because of no clear secure boundary. The nodes have the freedom to join and leave inside the network. Node can link a network involuntarily if the network is in the wireless scope of the node, therefore it can communicate with other nodes in the network. As a result of no secure boundaries, MANET is more at risk to attacks. The attacks may be passive or active, information leakage, forged message respond, denial of service or change in the integrity of data. The nodes are compromised and are subject to different attacks. There is no safety against attacks like firewalls or access control which results in exposure of MANET to attacks. Spoofing of node's identity, tempering of data, private data leakage and impersonating node are the results of such attacks when security is compromised.

- *Compromised Node:*

Some attackers get access inside the network so as to get control over the node in the network by means of unfair way to carry out their malicious activities. Mobile nodes in MANET are autonomous which means that they are free to move, enter or exit the network. This autonomous factor of mobile nodes makes it hard for the nodes to prevent malicious activity with which it is communicating. Ad-hoc network mobility makes it easy for a compromised node to alter its position time and again making it more complicated and difficult to track the malicious action. It is observed that the attacks from compromised nodes inside the network are more dangerous than those attacking from outside the network.

- *No Central Management:*

MANET is a self-configurable network where the communication among these mobile nodes is made with no fundamental control. The node work as a router and forwards and receives packets. MANET does not have an existing infrastructure. Decentralized management makes MANET more exposed to attacks. It becomes complicated to monitor the traffic and identify the threats in a dynamic and large scale Ad-Hoc network. Hence there should be a central entity taking care of the network by applying proper security about which node should join and which should not. The node join with each other on the account of blind mutual trust, which is managed by central entity by applying a filter on the nodes for finding out the suspicious one allowing the other nodes to know which node is suspicious one.

- *Problem of Scalability:*

In conventional networks, the network is built and each machine is connected to another machine through wire. The extent of the network and its topology is defined during its designing and this does not alter greatly during its lifetime. Alternatively we can say that the scalability of the network is proposed in the creation phase of the designing of the network. The case is rather opposite in MANETs as the nodes are mobile and because of this mobility in MANETs, the scale of the MANETs is varying. It is very tough to recognize and guess the numbers of nodes in the MANETs in the future. The nodes are liberated to move inside and outside of the Ad-Hoc network making the Ad-Hoc network greatly scalable and shrinkable. Due to this feature of the MANET, the services and all the protocols which MANET provides must be flexible to such changes.

IV. ROUTING PROTOCOLS

Due to the dynamic behaviour of a mobile ad hoc network numerous frequent and random changes in network topology are observed which increases the difficulty and complexity of routing among the mobile nodes. Therefore, the significance of routing protocol in establishing communications between the mobile nodes creates routing area the main dynamic research area within the MANET domain. Various routing protocols and algorithms were proposed and their performance under various network surroundings and traffic circumstances were studied and compared.
MANET routing protocols are basically divided into three categories: Proactive, Reactive and Hybrid.

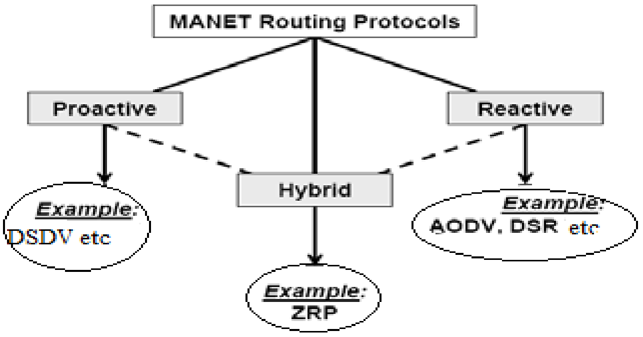

Fig.2. Classification of MANET Routing Protocol

- *Proactive Protocols:* Proactive is also known as table-driven routing protocol. In proactive routing, each node maintains one or more table to store routing information and every changes in network topology needs to be reflected by propagating updates right through the network so as to keep up a consistent network view. Examples of these schemes are the conventional routing schemes: Destination sequenced distance vector (DSDV). They maintain a reliable and up-to-date routing information for the entire network. It reduces the delay in communication and permits the nodes to rapidly verify which nodes are accessible in the network.

- *Reactive Protocols:* Reactive routing is also called as on-demand routing protocol because they do not sustain routing information or routing action at the network nodes when there is no communication. When a node in transmits a packet to another one, this protocol search the route in an on-demand way and establishes the connection so as to send out and receive the packet. The route discovery takes place by flooding the route request packets all through the network. Some the of reactive routing protocols are the Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR).

- *Hybrid Protocols:* They bring in a hybrid model that is a combination of reactive and proactive routing protocols. The Zone Routing Protocol (ZRP) is a hybrid routing protocol that divides the network into zones. ZRP gives a hierarchical architecture where every node maintains an extra topological information which requires added memory.

Ad-hoc On Demand Multipath Distance Vector (AOMDV)
Ad-hoc On-demand Multi path Distance Vector Routing (AOMDV) protocol is an expansion of the AODV protocol which computes several loop-free along with link disjoint paths. The routing entries for every destination contain a list of next-hops together with their hop counts. Sequence number of each next hop is same which helps in keeping track of the route. For every destination the node maintains the advertised hop count. The maximum hop count for all the paths that is used to transfer route advertisements of the destination is termed as advertised hop count. The route advertisement copy received by each node defines an alternate path to the destination. By accepting alternate paths to destination freedom of loop is guaranteed but the hop count for that destination is less than the advertised hop count. Consequently when the maximum hop count is used, the advertised hop count does not change for the same sequence number. Once the route advertisement for a destination is

received along with a larger sequence number, the next-hop record and the advertised hop count are reinitialized. Node-disjoint or link-disjoint routes are detected by the AOMDV. To detect node-disjoint routes, the duplicate RREQs are not rejected instantly by the nodes. A node-disjoint way is defined by every RREQs passing through a different neighbor of the source. The two RREQs incoming at an intermediate node which is passing through a different neighbor of the source should not traverse the similar node as they are not broadcasting the duplicate replicas. To acquire multiple link-disjoint paths, the destination replies to fake RREQs. The destination replies to the incoming RREQs only by means of exceptional neighbors. The RREPs pursue the reverse path after the first hop, which are node disjoint and hence link-disjoint. The trajectories of every RREP might overlap at an intermediate node. However each takes a diverse reverse path to the source to make sure link disjointness. The benefit of using AOMDV is that it still permits the intermediate nodes to reply to RREQs by selecting disjoint paths. However AOMDV has extra message overheads throughout the route discovery because of increased flooding. Since it is a multipath routing protocol, the destination replies to the multiple RREQs which results in longer overhead.

V. CLASSIFICATION OF SECURITY ATTACKS

The attacks are grouped into two types on the basis of the behaviour of the attack. They are Passive attack and Active attack

- *Passive attacks:* Passive attacks are those wherein the attacker indulges in eavesdropping or monitoring of data transmission. In other words, we can say that the attacker aims to obtain transit information. The term passive means that the attacker does not perform any modifications to the data. This is the reason that passive attacks are harder to detect. Hence to deal with passive attack we need to think about prevention instead of detection or corrective actions.

- *Active attacks:* In contrast to passive attack, the active attacks are based on the modification of the original message in some manner or the creation of a forged message. Therefore the prevention of these attacks are difficult. However attempts can be made to recover from them. These attacks can be in the form of modification, interruption or fabrication.

The features of MANETs make them prone to numerous new attacks.

- *Black Hole Attack:* In this type of attacks, malicious node claims to have an optimal path to the node as soon as it receives RREQ packets and sends the RREP along with the highest destination sequence number and minimum hop count value to the source node with whom RREQ packets wants to intercept. In fig.3 when node "S" wants to transmit data to destination node "D", the process of route discovery is initiated. On receiving the route request the malicious node "M" immediately sends the response back to the source node. If reply from node "M" is the first to the reach the source node then the source node "S" ignores all the reply messages from the other nodes and starts sending packets using route node "M". Consequently, all data packets are either consumed or lost by the malicious node.

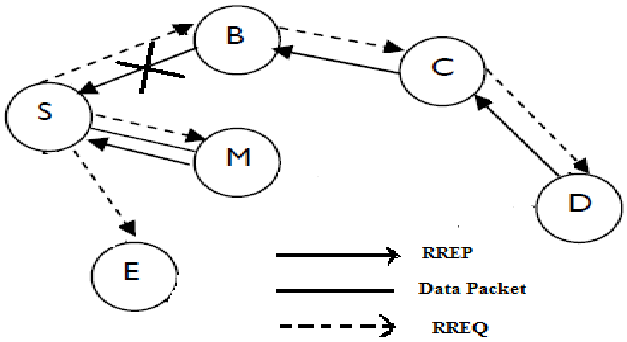

Fig3. Black Hole Attack

- *Gray hole Attack:* In this category of attack the attacker give the wrong impression about the network by assenting to forward the packets in the network. The moment it receives the packet from the adjacent node, the attacker drops the packets. This type of attack is an active attack. Primarily the attacker node behaves normally and sends true RREP messages in return to the nodes that sent RREQ messages. After it receives the packets it begins with dropping the packets and start on Denial of Service (DoS) attack. It drops packets at as well as forwards them in the network at the same time. Gray Hole attacks the attacker node and performs maliciously for the time the packets are dropped and thereafter switch to their normal performance. Node misbehaving attack is another name for this attack.

- *Wormhole attack:* In this type of attack, the attacker places themselves in strong calculated location in the network. They acquire the shortest path between the nodes as shown in the Fig.4. They promote their path in such a manner that the other nodes in the network think that they have the shortest path for the transmission of their data. A tunnel is created by the wormhole attacker with the intention that it can trace the ongoing communication and traffic at one network position and then channel them to some other positions in the network [12].Then the attacker node creates a direct link among each other in the network. The wormhole attacker at one end receives the packets and transmits these packets to another end of the network. The attackers in such positions are recognized as out of band wormhole. When an overlay tunnel is built by the attacker over the existing wireless medium the attack is recognized as in band wormhole attack. This attack is possibly more harmful and is one of the most preferred selections for the attacker.

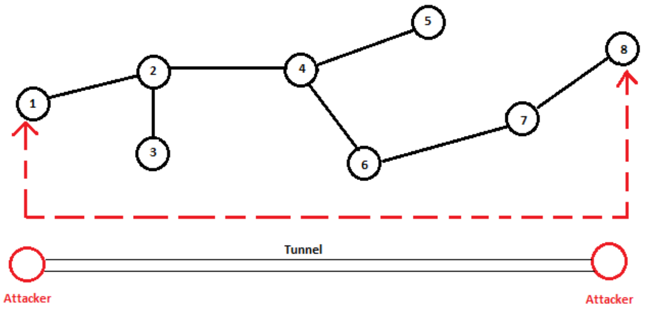

Fig.4 Worm Hole Attack

VI. CONCLUSION

MANETS are gaining popularity gradually as users prefer to connect to a network irrespective of their geographical position. Because of this exceptional feature of MANETs, they are open to a huge amount of malicious activity. Black Hole attack is one kind of threat in MANETs in which the data of the network is routed towards a node which drops all the packets entirely. In my next paper, a proposal for a feasible solution for black hole will be made which would be implemented using AOMDV protocol.

REFERENCES

[1]. C.E.Perkins and E.M.Royer, "Ad-Hoc on Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.

[2]. C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[3]. Z.J.Hass, M.R.Pearlman, P.Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", 55th Proceeding of International task force, July, 2002.

[4]. S. Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, Y.Nemoto, "Detecting Blackhole Attack on AODV- Wireless sensor Networks by Dynamic Learning Method", International Journal of Network Security, Vol. 5, No.3, pp. 338-346, Nov, 2007.

[5]. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding Royer, "Secure routing protocol for Ad-Hoc networks", In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Computer Science, California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, Nov. 2002.

[6]. H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless Ad-Hoc networks", Cincinnati Univ.,OH, USA; IEEE Communications Magazine, , Vol.40, pp.70- 75, ISSN: 0163-6804, Oct. 2002.

[7]. M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks", Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[8]. Zhu, C. Lee, M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols", IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.

[9]. H.L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on System and Networks and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), pp.149-149, April, 2006.

[10]. West off, D., Paul K, "Context Aware Detection of Selfish Nodes in DSR based Ad Hoc Networks", IEEE GLOBECOM.Taipei, Taiwan, pp. 178-182, 2002.

[11]. Y.F.Alem, Z.C.Xuan, "*Preventing Wormhole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",* 2ndInternational Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May,2010.

[12]. M.Parsons, P.Ebinger, "*Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc Networks*" April. 10, 2010.

[13]. Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, "*A Review of Current Routing Attacks in Mobile Ad Hoc Networks",* International Journal of Computer Science and Security, pp. 18-29, Volume-2 Issue-3, 2009

[14]. Mr. L Raja, Capt. Dr. S SanthoshBaboo "Comparative study of reactive routing protocol AODV, DSR, ABR and TORA" in International Journal Of Engineering And Computer Science Vol 2 Issue 3 March 2013 Page No. 707-718

[15]. C.Sivaram murthy, B.S. Manoj, *Adhoc wireless networks: Architectures, and protocols*, Pearson Education, 2004.

[16]. Aarti and Dr. S.S Tyagi, *"Study of MANET: Characteristics, Challenges, Application and Security Attacks",* IJARCSSE International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, May 2013

[17]. Mohit Kumar and Rashmi Mishra —*An Overview of MANET: History, Challenges and Applications*‖, Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012.

[18]. Dr. Kamaljit I. Lakhtaria, *Analyzing Reactive Routing Protocols in Mobile Ad Hoc Networks, Int. J. Advanced Networking and Applications* Volume:03 Issue:06 Pages:1416-1421 (2012) ISSN : 0975-029

[19]. Sunil Taneja and Ashwani Kush, —A *Survey of Routing Protocols in Mobile Ad-Hoc Networks*‖, International Journal of Innovation Management and Technology, Volume 1, No3, 279-285, August 2010.

[20]. Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao " *A survey of black hole attacks in wireless mobile ad hoc networks"* Human-centric Computing and Information Sciences 2011.