ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

Review on Mobile Ad Hoc Network Jamming Attacks

Anjali Sharma[1], Mr. Ranjan Kumar Singh[2],

M-Tech Student[1], HOD.[2] & Department of ECE & Shri Ram College of Engg. & Mgmt
Palwal, Haryana, India

A MANET is a set of nodes that do not depend on a pre-specified infrastructure to hold the network linked Wireless sensor networks are being utilized in various applications i.e. military purposes, health monitoring and home automation. These networks are fitted with huge no. of sensors, which are spatially scattered. Wireless sensor networks are broadly utilized in remote areas, defense and military scenarios. Thus, their security is severe issue. They are more susceptible to attacks as compared to wired networks. Wireless sensor networks endure from several active and passive attacks. This paper surveys security issues on Ad-hoc network and Ad hoc On-Demand Distance Vector (AODV) protocol Based on the attack interaction nature, the attacks against MANET can be categorized as active and passive attacks. Intruders against a network may be categorized into two groups: insider and outsider. While an outsider attacker is not a legitimate subscriber of the network, an insider attacker is an authenticated node and a part of the routing technique on MANETs.

Keywords: MANET, DSR, DoS, AODV,

I. INTRODUCTION

A wireless computing network is a computing network with no physical cable linked to each other. There are two types of mobile wireless network [2]: the infrastructural network and the Ad-hoc network. An infrastructural network is described as extend an available wired LAN to wireless devices by offering a BS. Every mobile client links to and interacts with the closest base station which is inside its communication radius. An Ad-hoc network is one in which a LAN is generated by wireless devices themselves without a static BS. The network is self-managed and peer-to-peer. All nodes are able of movement and can be linked dynamically. Each node can behave as, and is ready to behave as, a route to an external network at any moment. A Mobile Ad hoc Network (MANET) contains a loosely linked domain of routers. Generally called Mobile Packet Radio, Mobile Ad-hoc Network (MANET) technology has been a significant military research field. This can be carried out in practical usage whenever a local network with no static infrastructure is required. Other uses involve rescue operation and sensor networks. The support of these civilian and military utilizes usually needs the availability of a database to record and transfer severe mission information i.e. inventories and tactical information.Conventional mobile networks include the server in all data communication. MANET involves the conventional database abilities of data pull and data push, but it also permits the clients to interact directly with each other without the server involvement, unless essential for routing. Mobile ad hoc networks (MANETs) are more vulnerable to attacks because of the lack of infrastructure. Characteristics i.e., dynamic topological changes, open medium, distributed cooperation, limited bandwidth and restrained energy resources are some of the feature that build MANETs more susceptible.

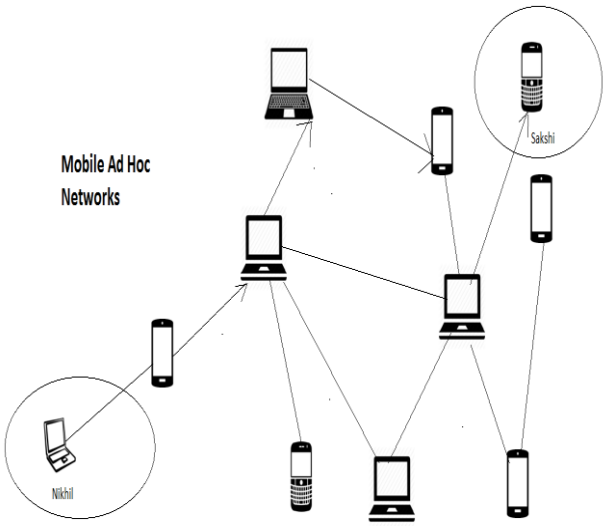

Figure 1: Mobile Ad Hoc Network

II. JAMMING ATTACKS

Jamming takes place when DoS attack that disrupts with the communication among nodes. The aim of the antagonist causing a jamming attack is to prevent legitimate receiver or sender from transferring or obtaining packets. Antagonists can launch jamming attacks at several layers of the protocol suite. In this work, we concentrate on attacks at the MAC and physical layer that result in collisions in the wireless network. Physical jamming is established by seamless transmissions and/or by causing packet collisions at the recipient. Virtual jamming takes place at the MAC layer by

attacks on data frames or control frames in IEEE 802.11 protocol. We explained the attack models in the following sections.

2.1 Physical Jamming (Physical Layer)

Physical or Radio jamming in a wireless medium is a simple but interruptive form of DoS attack. These attacks are created either by seamless emission of radio signals or by forwarding random bits onto the channel. The jammers causing these attacks can refuse complete access to the channel by monopolizing the wireless channel. The nodes attempting to interact have an unusually large carrier sense time waiting for the channel to become idle. This had an adverse propagating impact as the nodes enter into large exponential back-off periods.

2.2 Virtual Jamming (MAC Layer)

In IEEE 802.11 based MAC protocols, virtual carrier sensing is utilized at the MAC layer to determine the existence of the wireless medium. Jamming can be established at the MAC layer through attacks on the CTS/RTS frames or DATA frames. An important benefit of MAC layer jamming is that the antagonist node takes less power in intending these attacks in comparison of the physical radio jamming. Here, we concentrate on DoS attacks at the MAC layer resulting in collision of DATA frames or CTS/RTS control frames.

2.2.1 RTS/CTS Collision Attack (MAC Layer)*:*

In this attack model, the primary aim of the antagonist is to randomly interrupt network transmissions by colliding with RTS/CTS control frames. Seamless collision of RTS frames refuses channel existence to genuine network nodes. Since, it is complex to predict the RTS transmission period, the antagonist requires to transfer seamlessly same as physical jamming to increase the network interruption.

2.2.2 DATA Collision Attack (MAC Layer): In IEEE 802.11 MAC protocol, whenever a node transfers a CTS or RTS, all nodes in its transmission range defers their transmissions. Since, when a node A attempts to interact with another node B, a malicious node X in the recipient range can jam the channel by disrupting the radio transmission. The antagonist can hence launch a DATA collision attack by not adhering to IEEE 802.11 MAC protocol rules and transferring a packet during an on-going transmission.

2.3.1 Direct Collisions

In 802.11, distributed coordination function makes capable the nodes to access the channel randomly. This increases the probability that two nodes may start transmission simultaneously. However the packet transmissions begin at the same time, packets overlap and cause collisions at the recipient.

2.3.2 Hidden Terminal Collisions*:*

Carrier sensing multiple access with collision avoidance (CSMA/CA) is generally utilized in wireless networks to sense the wireless channel first before transmission for avoiding collisions with other transmitting nodes. Collision may however takes place because of hidden terminal issues, where a sender's transmission stays outside the geographical transmission coverage range of another node transferring in the recipient range.

2.1 RTS/CTS Collision Attack (MAC Layer)*:*

In this attack model, the primary aim of the antagonist is to randomly interrupt network transmissions by colliding with CTS/RTS control frames. Seamless collision of RTS frames refuses channel existence to genuine network nodes. However, it is complicated to predict the RTS transmission period, the antagonist requires to transfer continuously same as physical jamming to increase the network interruption.

2.2.2 DATA Collision Attack (MAC Layer):

In IEEE 802.11 MAC protocol, whenever a node transfers a CTS or RTS, all nodes in its transmission range defers their transmissions. Since, when a node A attempts to interact with another node B, a malicious node X in the recipient range can jam the channel by disrupting the radio transmission. The antagonist can hence launch a DATA collision attack by not adhering to IEEE 802.11 MAC protocol rules and transferring a packet during an on-going transmission.

2.3 Challenges in Detecting Collisions in Wireless Networks

Unlike wired Ethernet, collision detection is complex in wireless networks. however collision takes place at the recipient and not as MACA and 802.11 utilize RTS/CTS handshaking technique to resolve the collisions because of these hidden terminal nodes. Since, research represents that even with CTS/RTS handshake, 802.11 based MAC protocols do not entirely solve the hidden terminal issues because of large interference range. Furthermore, because of their important overhead in mobile ad hoc networks, CTS/RTS handshake I usually disengaged from the MAC protocol operation resulting in higher collisions.

2.3.3 Network Congestion*:*

Congestion in 802.11 networks is because of high usage of the shared wireless medium by the nodes. The congestion state is usually caused because of heavy traffic load from few nodes in the channel or high density of nodes competing for channel access to transfer data. When there is a large no. of subscribers in the network, collisions are more frequent. Such collisions because of channel contention and traffic load can reduce the network performance to a large extent.

We realize from the above specified factors that, in 802.11 based wireless ad hoc network, packet collisions may take place either because of intentional jamming attacks or as a consequence of inadvertent hidden terminal issues and network congestion. Thus, it is of utmost significance that appropriate consideration of several collision factors requires to be considered towards determining the existence of jamming attacks in the wireless channel.

III. VULNERABILITIES OF MANETS

Dynamic Topology*:* In MANETs, nodes can add and leave the network dynamically and can travel independently [2]. Because of this behavior there is no static set of topology operates in MANETs. The nodes with inadequate physical security may become malicious node and decrease the performance of network.

Wireless Links: As the nodes in these networks are interlinked by wireless interface that builds it highly vulnerable to connect attacks. The wireless networks bandwidths are less in comparison of wired networks, which attracts several intruders to prevent general communication between nodes.

Cooperativeness: In MANETs, all routing protocols consider that nodes offer secured communication. But some nodes may become malicious nodes which interrupt the network operation by modifying routing information etc [1].

Lack of clear line of defence: There is no clear line of defence technique existed in the MANETs; attacks can come from any directions. Intruders can attack the network either externally or internally.

Limited resources: The MANETs contains different set of devices i.e. computers, laptops, mobile phones etc. All of such devices having different processing speed, storage capacity, computational power etc. This may attracts the intruders to concentrate on new attacks.

IV. ROUTING INFORMATION USED IN PACKET FORWARDING

This class is categorized into two subclasses: topology-based and position-based routing protocols. In topology-based routing, every node should be informed of the network layout, also should capable to send packets utilizing information about existed nodes and connections in the network. In opposite, position-based routing should be aware of the nodes position in the packet sending.

4.1 TOPOLOGY-BASED ROUTING PROTOCOL

Topology-based routing protocol often a conventional MANET routing protocol, it utilizes connections information which recorded in the routing table as a basis to send packets from source node to destination node; it commonly classified into three classes (depending on underlying architecture) [3],[10]: Proactive (periodic), Reactive (on-demand) and Hybrid.

4.1.1 PROACTIVE ROUTING PROTOCOLS

Proactive protocols permit a network node to utilize the routing table to record routes information for all other nodes, every entry in the table consists the next hop node utilized in the route to the destination, without regarding of whether the route is actually required or not. The table must be maintained frequently to reflect the network configuration changes, and should be flood periodically to the neighbors. This mechanism may cause more overhead particularly in the high mobility network. Since, routes to destinations will always be existed when required [4]. Proactive protocols often based on shortest path algorithms to find which route will be selected; they basically utilize two routing mechanisms: Link state strategy and distance vector strategy.

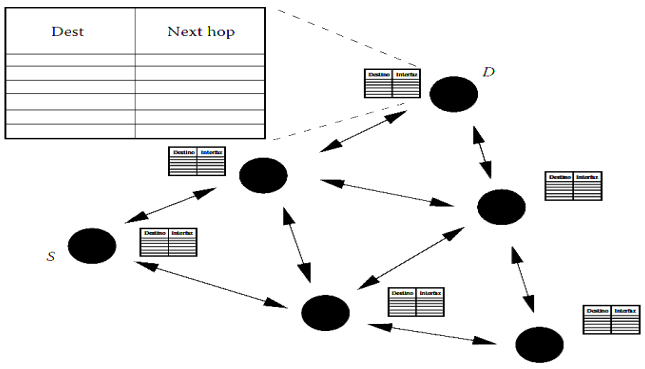

Figure 2. Proactive Routing Scheme

A. DESTINATION SEQUENCE DISTANCE VECTOR ROUTING (DSDV)

DSDV protocol it is an earliest ad hoc routing protocol, it applies the distance vector technique and utilizes a shortest path algorithm to implement only one route to destination node which recorded in the routing table, every routing table has information about all accessible network nodes, as well as the total no. of hops required to arrive these nodes, and every entry in the routing table is labeled with a sequence no. started by the destination node. To manage routes reliability, every node must periodically flood its routing table to its neighboring nodes. DSDV protocol ensures the loop free routes, excludes additional traffic caused by quick updates, as well as decreases control message overhead, it also holds only the optimum path to each node, instead of keeping multi paths which will support to decrease the total routing table size [8]. Since, DSDV increases the overhead in the huge network; due to unessential updating broadcast even if there is no change in the network configuration. Besides that, DSDV don't offer multi routes to destination node [8] and has no control over the network congestion which reduces the routing efficiency [11]. As the result of these restrictions, Randomized DSDV protocol (R-DSDV) is introduced to support congestion control over DSDV; by managing nodes randomized decision which permits every node to build a decision whether to send or drop a packet. Since, the R-DSDV generates more overhead in comparison of the DSDV protocol.

B. OPTIMIZED LINK STATE ROUTING PROTOCOL (OLSR)

OLSR protocol implements the link state technique; it holds a routing table consists of information about all possible routes to network nodes. Once the network configuration is changed every node must forward its managed information to some chosen nodes, which retransfer this information to its other chosen nodes. The nodes which are not in the chosen list can just read and process the packet [10].

Some researchers believe that OLSR has easy process which permits it to built-in different operating systems, besides it operates well in the dynamic configuration, also it is normally appropriate for applications that need low latency in the data transmission (i.e. warning applications) [11]. Since, OLSR may lead network congestion; due to frequent control packets which forwarded to manage configuration changes, furthermore OLSR neglect the high resources abilities of nodes (i.e. bandwidth, transmission range, directional antenna and so on) [12]. Thus, some researchers introduce Hierarchical Optimized Link State Routing (HOLSR) protocol as improvement of the OLSR protocol, which reduces routing control overhead in the large size networks, also increases the routing performance; by the describing network hierarchy architecture with several networks [13]. Also some researchers introduce QOLSR as a solution of offering a path such that the existed bandwidth at every node on the path is not less than the needed bandwidth. QOLSR assumes delay as a second for path selection [12]. These protocols often offer average improvement for the packets QoS. Since, they cause more complexity, increasing packet overhead, and only appropriate for some restricted applications [9].

4.1.2 REACTIVE ROUTING PROTOCOLS

Reactive routing protocols (also known as on-demand) decrease the network overhead; by managing routes only when required, that the source node initiates a route discovery procedure, if it requires a non available route to a destination node, it does this procedure by broadcasting the network by a route request message. After the message arrives the destination node (or to the node which has a route to the destination node), this node will forward a route reply message back to the source node utilizing unicast communication [17]. Reactive routing protocols are suitable to the mobile ad hoc networks large size which has highly mobility and frequent configuration changes [18]. Several reactive routing protocols have been formulated, the following sections will present feature of some reactive protocols, as well as represents the available improved protocols.

A. AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV routing protocol is introduced for mobile ad hoc network, it has been measured in various researches and presents good results as compared to related routing protocols; so it has a good documentation [19]. AODV provides low network overhead by decreasing messages broadcasting in the network in comparison of proactive routing protocols, besides decreasing the need of memory size; by decreasing the routing tables which hold only entries for current active routes, also holds next hop for a route instead of the entire route. It also offers dynamically updates for following the route conditions and removes looping in routes; by utilizing destination sequence no. So AODV is reliable to highly dynamic network configuration and large-scale network [20]. Since, it causes large delays in a route finding, also route failure may need a new route discovery which creates extra delays that reduce the data transmission rate and increase the network overhead [17]. Furthermore, the redundant floods without control will consume additional bandwidth (broadcast storm issue), this issue increases as the no. of network nodes increases, that besides collisions which yield to packet lost issue [19].

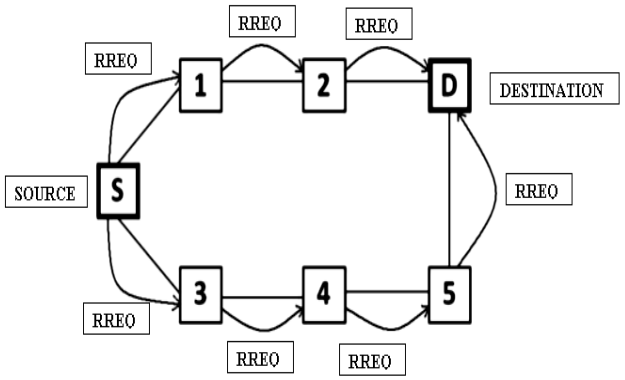

Figure 3. Route Request Reactive Routing

There are various protocols have been introduced to improve AODV protocol; by reducing its problems.

B. DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

DSR protocol objectives to offer a highly reactive routing procedure; by implementing a routing technique with an extremely low overhead and fast reaction to the quick network changes, to ensure successful data packet delivery without regarding of network changes. DSR is a multi hop protocol; it reduces the network overhead by decreasing periodic messages. This protocol has two main phases: route discovery and route Maintenance. In the route discovery phase, when a source node requires an un-existed route, it starts broadcasting a route request message. All intermediary nodes which obtained this message will re-flood it, except if it was the target node or it has a route to the destination node; in this case the node will forward a route response message back to the source, later the obtained route is cashed in the source routing table for future usage. If a route is failing, the source node will be reported by a route error message. In DSR protocol, each data packet has a entire list of the intermediary nodes; so the source node should remove the failed route from its cache, and if it records other successful route to that destination node in its cache, it will interchange the failed one by the other successful route. But if there is no alternative route, it will start a new route discovery procedure [27]. The advantage of DSR protocol is clearly represented in a network with low mobility; because it can utilize the alternative route before initiates a new procedure for route discovery. Since, the multi routes may yield to extra routing overheads by appending all route information to each data packet, besides, as the network span larger distance and involving more nodes, the overhead will quickly increase and as result network performance will be reduced [28].

V. CONCLUSION

Nowadays, Security is a severe issue in the area of computer networks. They are more susceptible to attacks and we have enhanced the quality and issues in Mobile Ad-hoc network and routing protocols. As jamming is a very critical attack to the normal operation of wireless networks, currently much research has been performed to deal with it. All mechanisms are good from their perspective but not best from all points. Mechanisms explained in this paper that can offer information about security functions and an overall visual check, which might be appropriate in some applications. But, there is also requirement to simulate a specific scenario to visualize the impact of without and with Jamming attack for the improved routing protocol.

REFERENCES

[1] Sabbar Insaif Jasim," Jamming Attacks Impact On the performance of Mobile Ad-Hoc Network and Improvement Using MANET Routing protocols," International Journal of Engineering and Advanced Technology(IJEAT), Volume 3, Issue 2, Dec. 2013, pp. 325-330.

[2] Ajana J., Helen K.J, "Mitigating Inside Jammers in MANET Using Localized Detection Scheme", International Journal of Engineering Science Invention, Volume 2, Issue 7, July 2013, pp. 13-19.

[3] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar," Improving Reliability of Jamming

Attack Detection in Ad-Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS) , Vol. 3, No.1, April 2011, pp. 57-66.
[4] S. Raja Ratna, R. Ravi and Dr. Beulah Shekhar," Mitigating Denial of Service Attacks in Wireless Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, No.5, May 2013, pp. 1716-1719.
[5] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, "Study of Different Attacks on Multicast Mobile Ad hoc Network", Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.
[6] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.
[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.
[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.
[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.
[10] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.
[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7
[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, "Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis", Military Communications Conference, October 2006, pp. 1-7.
[13] Mani Arora, Rama Krishna Challa and Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, 2010, pp. 102-104
[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.
[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.
[16] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference, 2005.
[17] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005
[18] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.
[19] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003