Available online at www.ijiere.com
International Journal of Innovative and Emerging Research in Engineering
e-ISSN: 2394 - 3343 p-ISSN: 2394 - 5394

Survey of Various Attacks against Wireless ad hoc networks

Mr. Margam K. Suthar[a]
[a]Assistant Professor, Post Graduate Research Centre for Mobile Computing and Wireless Technologies, Gujarat Technological University, Chandkheda, Ahmedabad-382424.Gujarat. (India)
margam.19ec@gmail.com

ABSTRACT:
Today wireless communication technique has become an essential tool in any application that requires communication between one or more sender(s) and multiple receivers. The wireless ad hoc network is very common today, but the main issue is the security. There are many solution provided by different researcher but still faces research challenges. In MANET, nodes have limited resources like bandwidth, battery power and storage capacity.
Since multiple users can use this technique simultaneously over a single channel, security has become a huge concern. Even though there are numerous ways to secure a wireless network and protect the network from numerous attacks, providing 100% security and maintaining confidentiality is a huge challenge in recent trends. This paper will present you a survey about the various threats to wireless networks, the various advancements in securing a network and the various challenges in implementing the same.

Keywords: Ad hoc Networks, Routing Protocols, AODV (Ad-hoc On-demand Distance Vector), AWK (Aho Weinberger Kernighan), ACK (Acknowledgement), DSDV (Destination Sequence Distance Vector)

I. INTRODUCTION

Communication being a mode of sending and receiving information is gaining more popularity in today's world. There are various modes of communication one of them is wireless mode; in which communication takes place through an open medium [1]. There are various types of wireless networks. These are cellular networks, satellite networks and ad hoc mobile networks. Amongst the wireless networks 802.11 networks are the most popular. Wireless 802.11 networks can be categorized into two types: Infrastructure and Ad-hoc mode. Infrastructure based networks have a fix Backbone [1]. An ad-hoc network is a collection of nodes which can communicate with each other without any infrastructure. Wireless medium is a medium which can be accessed by both legitimate users and attackers. End users and corporations are heavily interested in taking the advantage of this wireless medium, but this also comes with some security issues [2].

Ad-hoc networks are a collection of mobile nodes that can be deployed without the need for any centralized infrastructure. Ad hoc network is very flexible and can configure itself automatically. Ad hoc networks are the voice/data networks that are established temporarily without requirement of an infrastructure, in which some of the network devices are a part of the network only for the duration of a communication session.

II. ADHOC NETWORK

Wireless LANs can be classified based on their mode of operation such as either infrastructure or ad-hoc. Infrastructure mode has a fixed wired backbone for communicating with each other; whereas the ad-hoc mode doesn't rely on a backbone. An ad hoc network can be formed when a group of mobile devices communicate with each other without depending on any fixed infrastructure. In such cases, neighbouring nodes communicate with each other's while communication between non-neighbour nodes is performed via the intermediate nodes that can act as routers. The network topology also frequently changes in ad-hoc network. Ad-hoc wireless networks are prone to route breaks that can result due to various sources such as node mobility, signal interference, high error rate and packet collision [2].

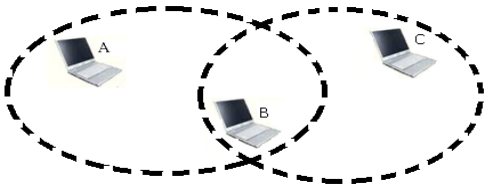

Figure 1: ad hoc network [3]

The figure 1 explains the ad hoc network wherein there are three nodes A, B and C. Node A and Node B are in the range of each other. Similarly node B and C are in range of each other. If node A wants to send some data to node C it has to pass through the intermediate node b so node B acts as a router. Here comes the main operation of routing in ad hoc network [2].

III. ATTACK TYPES IN AD HOC NETWORK

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. These attacks are categorized in previous chapter "security issues in MANET" on the basis of their nature.

A. Passive Eavesdropping

An attacker can listen to any wireless network to know what is going on in the network. It first listens to control messages to infer the network topology to understand how nodes are located or are communicating with another. Therefore, it can gather intelligent information about the network before attacking. It may also listen to the information that is transmitted using encryption although it should be confidential belonging to upper layer applications.

Eavesdropping is also a threat to location privacy [3]. An unauthorized node can notice a wireless network that exists within a geographical area, just by detecting radio signals. To combat this, traffic engineering techniques have been developed.

B. Selective Existence (Selfish Nodes)

This malicious node which is also known as selfish node and which is not participating in the network operations, use the network for its advantage to enhance performance and save its own resources such as power. To achieve that, selfish node puts forth its existence whenever personal cost is involved. Therefore these selfish node behaviour are known as selective existence attacks. [3]. For instance, selfish nodes do not even send any HELLO messages and drop all packets even if they are sent to itself, as long as it does not start the transmission. When a selfish node wants to start a connection with another node, it performs a route discovery and then sends the necessary packets. When the node no longer needs to use the network, it returns to the "silent mode" After a while, neighbouring nodes invalidate their own route entries to this node and selfish node becomes invisible on the network [4].

Actually, dropping packets may be divided into two categories according to the aims of the attacking node. Attacker may want to drop the packets of only the other nodes that it will attack later. To do that it must look at the packet to see whether it comes from this node. If attacker looks at the content of all packets aggregating from the network, it spends CPU resource and naturally battery life. This is not desirable behaviour for selfish nodes because it spends battery life. Therefore attackers are not interested in the content of the packets if its aim is not to consume its own resources. First category of dropping packets cannot be evaluated as a selfish node behaviour. Thus selectively dropping message is not a selfish node behaviour mentioned in [4]. Selective existence is kind of a passive attack, nodes just do not participate in the network operations and they do not change the content of packets.

C. Gray Hole Attack (Routing Misbehaviour)

Gray hole attacks is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack [5].

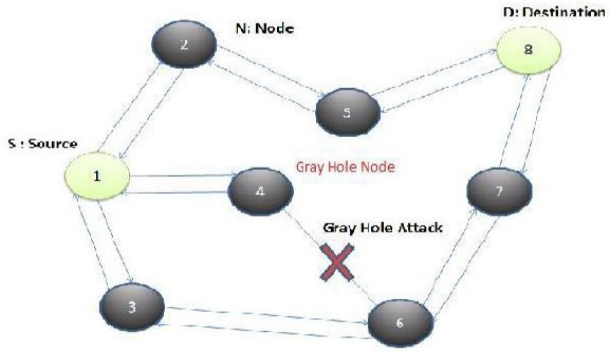

Figure 2: Gray Hole Attack [2]

The Gray Hole attack is a kind of Denial of Service (DoS) attacks. In this attack, an adversary first exhibits the same behaviour as an honest node during the route disc ovary process, and then silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. The malicious nodes could degrade the network performance disturb route discovery process [5].

D. Black Hole Attack

The difference of Black Hole Attacks [6] compared to Gray Hole Attacks is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the

routing table of the victim node, before other nodes send a true one [7]. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network [7].

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [8].

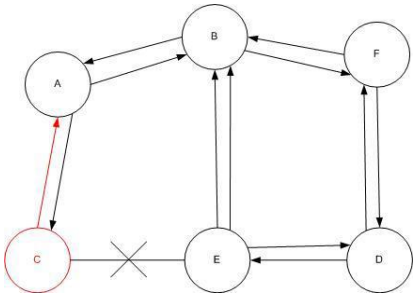

Figure 3: Black Hole Attack [4]

The method how malicious node fits in the data routes varies. Figure. 3 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

E. Modification Attack

The nature of Ad-Hoc network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack. Misrouting and impersonation attacks are two types of modification attack [9].

F. Misrouting Attack

In misrouting attack a malicious node which is part of the network, tries to reroute the traffic from their originating nodes to an unknown and wrong destination node [10]. As long as the packets remain in the network make use of resources of the network. When the packet does not find its destination the network drops the packet.

G. Impersonation Attack

Due to lack of authentication in ad-hoc networks, only MAC or IP addresses uniquely identify hosts. These addresses are not adequate to authenticate the sender node. Therefore non-repudiation is not provided for ad-hoc network protocols. MAC and IP spoofing are the simplest methods to pretend as another node or hide in the network [10]. Impersonation attack is also called spoofing attacks in which a malicious node uses IP address of another node in outgoing routing packets. The aims of impersonation attacks to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key private key or even password of the nodes [11].

A defective node or an opponent may present multiple identities to a peer to peer network in order to appear and function as distinct node. By becoming part of the peer to peer network the opponent may then overhear communication [11].

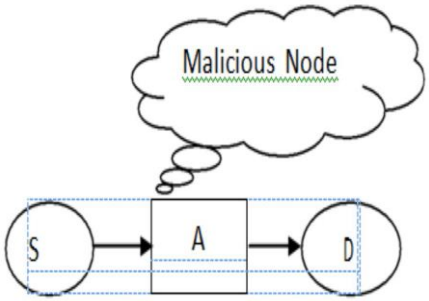

Figure 4: Impersonate Attack [4]

The introduction of impersonation attack in any network there is a reduction of throughput in the network. Packet delivery ratio also drops and there is an increases checksum error and packet loss ratio.

In above figure S is the source and D is destination and A is intermediate node. Another node that is malicious node replaced its identity with intermediate node and hides its actual identity with other nodes. So when source send any message to other nodes within the network then that malicious node also get that message and misused all the information Impersonation attack is main cause of colluding attack in which compromised node injected malicious node in to the network and make number of replicated copy of malicious node for doing future attacks in overall network [12].

H. Attack Against The Routing Tables

Every node has its own routing table to find other nodes easily in the network. At the same time, this routing table draws the network topology for each node for a period (max. 3 seconds, duration of ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol). If malicious node attacks against this table, attacked nodes do not find any route to other nodes whom it wants to connect. This attack is always performed by fabricating a new control message. Therefore it is also named fabricating attack [12].

I. Wormhole Attack

In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point.

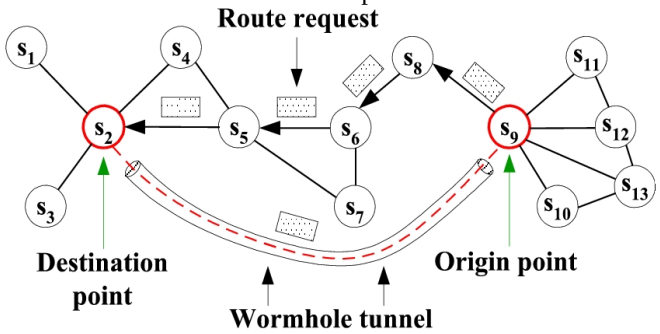

Figure 5: Wormhole Attack [8]

An attacker intrudes communications originated by the sender, copies a portion or a whole packet, and speeds up sending the copied packet through a specific wormhole tunnel in such a way that the copied packet arrives at the destination before the original packet which traverses through the usual routes. Such a tunnel can be created by several means, such as by sending the copied packet through a wired network and at the end of the tunnel transmitting over a wireless channel, using a boosting long-distance antenna, sending through a low-latency route, or using any out-of bound channel.

J. Flooding Attack

The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

K. Sleep Deprivation Torture Attack (Battery Exhaustion)

One of the most interesting attack in MANETs, where the attacker tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep. This attack is known as sleep Deprivation torture attack. The nodes operating in MANETs have limited resources i.e. battery life, the node remain active for transmitting packets during the communication [14].When the communication cease these nodes go back to sleep mode in order to preserve their resources. The attacker exploit this point of the nodes by making it busy, keeping it awake so as to waste all its Energies and make it sleep for the rest of its life. When nodes went to sleep for ever an attacker can easily walk into the network and exploit rest of the network.

L. Sybil attack:

A single node presents itself to other nodes with multiple spoofed identifications (either MAC or network addresses). The attacker can impersonate other nodes identities or simply create multiple arbitrary identities in the MAC and/or network layer. Then the attack poses threats to other protocol layers; for examples, packets traversed on a route consisting of fake identities are selectively dropped or modified; or a threshold-based signature mechanism that relies on a specified number of nodes is corrupted [14].

M. Jellyfish Attack

In jellyfish attack, the attacker attacks in the network and introduce unwanted delays in the network. In this type of attack, the attacker node first get access to the network, once it get into the network and became a part of the network. The attacker then introduce the delays in the network by delaying all the packets that it receives, once delays are

propagated then packets are released in the network. This enables the attacker to produce high end-to-end delay, high delay jitter and considerably effect the performance of the network [15].

N. Routing Table Overflow Attack

Routing Table Overflow attack is usually done against proactive protocols. In this attack, non-existent node data is sent in the network, more ever corrupting and degrading the rate, when routing tables are updated. Proactive routing protocols updates route periodically before even they are required. This is one of the flaws that make proactive protocols vulnerable to the routing table attack. The attacker tries to create so many routes to nodes that do not exist in the network. This is done by using RREQ messages. The attacker sends RREQ messages in the network to non-existent nodes. The nodes under attack results its routing table full and doesn't have any more entry to create new. In other words the routing tables of the attacked nodes are overflow with so many route entries.

IV. CONCLUSION

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis, we have analysed the behaviour and challenges of security threats in mobile Ad-Hoc networks with solution finding technique. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes.

REFERENCES

[1] Sachin Dev Kanawat and Pankaj Singh Parihar "Attacks in Wireless Networks" IJSSAN 2011

[2] Prateek Suraksha Bhushan, Abhishek Pandey, and R.C. Tripathi of IIT Allahabad "A Scheme for Prevention of Flooding Attack in Wireless Sensor Network" ISSN: 2047-0037 (IJRRWSN)

[3] Alejandro Proano, Loukas Lazos of University of Arizona, "Selective Jamming Attacks in Wireless Networks"

[4] Wazir Zada Khan, Yang Xiang, Mohammed Y Aalsalem, Quratulain Arshad "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks" published on February 2011 in MECS.

[5] Yih-Chun Hu, Adrian Perrig and David B. Johnson, Members, IEEE "Wormhole Attacks in Wireless. Networks"

[6] K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi "Various Attacks in Wireless Sensor Network: Survey" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013

[7] Nidhi Gour1,Monika Agarwal2,Heena Singh3,Ajay Kumar,' A Review on Impersonation Attack in Mobile Ad-Hoc Network'International Journal of Computer Trends and Technology (IJCTT) – volume 8 number 1– Feb 2014

[8] H.L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr, 2006.

[9] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Neworks," International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[10] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[11] 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.

[12] 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.

[13] V.Mahajan, M.Natue and A.Sethi, "Analysis of Wormhole Intrusion attacks in MANETs," IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[14] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002. H.Deng, W.Li and D.P.Agrawal, "Routing Security in Wireless Ad-Hoc Networks," University of Cincinnati, IEEE Communication Magzine, Oct, 2002.

[15] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007

[16] 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 Comput. Sci., California Univ., Santa Barbara, CA, USA. Pp.78- 87, ISSN: 1092-1648, 12-15 Nov. 2002.

Margam K. Suthar was born in Visnagar, Gujarat in 1988. He received the B.E. degree in Electronic and Communication Engineering from Hemchandracharya North Gujarat University, Patan, in 2010, M.Tech degree in Electronic and Communication at Ganpat University, Kherva - 382711.Dist.Mehsana, Gujarat, India in 2012.

He has two year of teaching experience in the field of Electronic and Communication. He is currently an ASSISTANT PROFESSOR, POST-GRADUATE RESEARCH CENTER FOR MOBILE COMPUTING & WIRELESS TECHNOLOGIES at Gujarat Technological University (GTU), Visat - Gandhinagar Highway Chandkheda, Ahmedabad – 382424 – Gujarat, India. He has authored and published / presented six publications in reputed International Journals and Conferences. His research interests include Mobile Computing, Wireless Technologies, ad-hoc Network, and Congestion Control and improve TCP/IP protocol for High Speed Network & Wireless Network.