© 2019 IJSRSET | Volume 6 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET196646

A Study of Attack on Wireless Ad-Hoc Network

Pawitar Dulari
Department of Physics, Government P.G. College Una (H.P.), India

ABSTRACT

Security is an essential requirement in wireless ad hoc network. The type of ad hoc networks makes them vulnerable to distinct forms of attack. The random nature of these networks makes invoke of security a challenging issue. The paper shows the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks. Then it presents the main attack categories that exist in it. Finally presents the current security solutions for the mobile ad hoc network.

Keywords : MANET, Classification of Attacks, Security in MANET, Ad Hoc.

I. INTRODUCTION

The increase of cheaper, lesser and extra powerful mobile devices have made wireless Ad Hoc networks (MANET) [1, 2] to become one of the rapid growing areas of research. This new class of self-deploying network may accomplice wireless communication with huge degree point mobility. Dissimilar traditional wired networks they have no fixed framework.

Security in MANET is the most analytical burden for the elemental functionality of network. Opportunity of network services, confidentiality and integrity of the data can be brought out by assuring that security issues have been met. MANET often suffer from many security attacks because of its features admire open medium, changing its topology dynamically, cooperative algorithms, lack of central checking and management and no clarify defense mechanism. These elements have changed the action field position for the MANET against the security threats.

In recent years, security of computer networks has been widely been debate and formulized. Most of the discussions elaborated only static and networking occupied on wired systems. However, MANET still in need of more discussions and improvement in terms of security [5]. With the evolution of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the contrast of wired network MANET is distinct. The routing protocols constructed mainly for internet is distinct from the MANET. Traditional routing table was basically made for the hosts which are connected wired to a non-dynamic backbone [3].

Due to which, it is impossible to support MANET mainly as the movement and dynamic topology of networks. As different factors including a shortage of infrastructure, absence of before established faith relationship in between the definite points and dynamic topology, the routing protocols are vulnerable to different attacks [4]. Main vulnerabilities which have been so far analyzed are mostly these kinds which contain selfishness, dynamic nature, and severe resource constraint and open network medium. MANET work beyond a centralized administration where point communicates with everyone on the base of mutual trust. This distinctive makes MANET higher vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [4, 1]. Mobile points present within the range of wireless link can overhear and even participate in the network.

II. METHODS AND MATERIAL

A. Flaws in MANETS: MANETs are very flexible for the points i.e. points can freely join and leave the network. There is no main body that keeps watching on the points entering and leaving the network. All these weaknesses of MANET make it vulnerable to attacks and these are discussed below.

1) **Non Secure Boundaries:** MANET has no crystal clear secure perimeter, so it is vulnerable to many attacks. In MANET, points have the freedom to join and leave inside the network. A point can tie a network automatically if the network is in the radio range of that point, thus it can communicate with alternative points in the network. Appropriately it has no secure boundaries; MANET is more susceptible to attacks. The attacks in MANET may be passive or active, crack of information, bogus message reply, denial of service or altering the data integrity. The links are compromised and are open to various link attacks. Attacks on the link interfere betwixt the points and then invading the link, destroying the link later performing malicious behavior. In MANET there is no protection against attacks like firewalls or access control. Spoofing of point's identity, data tempering, confidential information leakage and impersonating point are the conclusions of such attacks when security is compromised [1].

2) **Compromised Node:** Some of the attacks are to make approach innards the network in order to get supervision over the node in the network using improper means to carry out their malicious activities. Mobile points in MANET are release to move, accompany or escape the network in more words the mobile point are autonomous [6]. As a result of this sovereign factor for mobile nodes it is very problematic for the nodes to avert malicious activity it is communicating with. Ad-hoc network mobility makes it accessible for a compromised node to adjustment its position so frequently making it more difficult and troublesome to track the Gupta et al., malicious activity. It can be detected that these hazard from compromised nodes innards the network is more dangerous than attacking hazards from outside the network.

3) **No Central Management:** MANET is an automatic configurable network, which subsist of Mobile nodes where the communication amid these mobile nodes is done without a significant control. Each and every node act as router and can forward and receive packets [7]. MANET works after any preceding framework. This scarcity of centralized management leads MANET higher vulnerable to attacks. Disclosing attacks and observing the traffic in huge dynamic and for broad scale Ad-Hoc network is very difficult due to no key management. When there is a central entity pay attention to the network by applying proper security, authentication which node can join and which can't. The node connect with one other on the ground of curtain mutual faith on each other, a central entity can manage this by applying a filter on the points to find out the suspicious one, and let the other points know which node is suspicious.

4) **Problem of Scalability:** In traditional networks, where the network is built and each machine is associated to the other machine with use of wire. The network topology and the scale of the network, while designing it is characterized and it do not alter enough during its life. Scalability of the network is

characterized in the starting stage of the designing of the network. But in MANETs the points are mobile and being their mobility in MANETs, the scale of the MANETs is reforming. It is too hard to know and predict the numbers of points in the MANETs in the future. The points are free to move in and out of the Ad-Hoc network which makes the Ad-Hoc network very much scalable and shrinkable. Observing this property of the MANET, the protocols and everyone the services that a MANET provides must be adaptable to such adjustments.

CLASSIFICATION OF ATTACKS

The attacks perchance classified on the ground of the origin of the attacks i.e. Internal or External, and on the essence of the attack i.e. Passive or Active attack. This allocation is critical because the attacker can accomplishment the network either as internal, external or along with active or passive attack across the network.

A. External and Internal Attack: External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending fake packets. This reduces the performance of the whole network. This attack similar to the attacks that are made against wired network. These attacks can be avoided by implementing security measures such as firewall, where the entry of unauthorized person to the network can be slaked. Where as in internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and then it starts its malicious behavior. Internal attack is more severe attacks then external attacks.

B. Active and Passive: Attack In active attack, the attacker downgrades the work of the network, abduct important information and try to damage the data during the exchange in the network. Active attacks can be an external or an internal attack. The active attacks destroy the performance of network. In this, the attacker point acts as internal point in the network. As point is an active part of the network it is easy for the point to exploit and hijack any internal point to use it to introduce fake packets injection or denial of service. The attacker can alter, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network [8]. In Passive attack, the attacker listen to the network in form to get information, what is going on in the network? By listening the network, the attacker know and understand how the points are communicating with each other and how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network.

ATTACKS IN MANET

A. Wormhole Attack: Wormhole attack is a threatening attack again routing protocols for the mobile ad hoc networks [9, 10]. In the wormhole attack, an attacker records packets (or bits) at one point in the network, tunnels them (possibly selectively) to some other location, and replays them there into the network. The replay of the information will make great chaos to the routing issue in mobile ad hoc network because the points that get the replayed packets cannot know apart it from the genuine routing packets. Furthermore, for tunneled distances longer than the normal wireless transmission range of an individual hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route, which makes the victim point be more likely to accept the tunneled packets instead of the genuine routing packets. The routing functionality in the MANET will be severely interfered by the wormhole attack. For example, most existing MANET routing protocols, without some mechanism to uphold against the wormhole attack, would be unable to find routes longer than one or two hops, badly disrupting communication.

Defense against Warmhole Attack: A Packet leash is a mechanism for disclosing and, thus defending against wormhole attacks. A leash is any information that is joined to a packet designed to restrain the packet's top allowed transmission distance. There are two particular leashes, and that are geographical leashes along with temporal leashes. A geographical leash provides that the recipient of the packet is within a convinced distance from the sender. A temporal leash assures that the packet has an uppermost bound on its period, which restrains the top travel distance. Geographical Lease or temporal lease either can protect the wormhole attack, because it allows the receiver of packet to detect if the packet traveled further than the leash allows. A geographical leash in conjunction with a signature scheme can be used to snap the attackers that bluff to endure at multiple locations: when a legitimate point overhears the attacker asking to be in particular locations that would only be possible if the attacker could travel at a velocity above the maximum point velocity v, the legitimate point can use the signed locations to convince other legitimate points that the attacker is malicious.

B. Rushing Attack: The rushing attack, which results in denial of services when used against all previously, published on-demand MANET routing protocol [3]. Rushing attack exploits this duplicate suppression mechanism by quickly forwarding route discovery packet in order to gain access to the forwarding group [5, 8]. When a point send a route request packet (RR packet) to another point in the wireless network, if there an attacker present then he will accept the RR packet and send to his neighbour with high transmission speed as compared to other points, which are present in the wireless network. Because of this high transmission speed, packet forwarded by the attacker will first reach to the destination point. Destination point will accept this RR packet and discard other RR packets which are reached later. Receiver found this route as a authenticroute and use for more communication. This way attacker will successfully gain access in the communication between sender and receiver.

C. Gray Hole Attack: In gray hole attack the attacker misguides the network by agreeing to forward the packets in the network. When it receive the packets from the neighboring point, the attacker drop the packets. This is a type of active attack. In the starting the attacker points behaves normally and reply true RREP messages to the points that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service attack. The malicious behavior of gray hole attack is distinct in different ways. It drops packets while forwarding them in the network. In some other gray hole attacks the attacker point behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [20]. Due to this behavior it's very difficult for the network to find out such kind of attack. Gray hole attack is further admitted as Node misbehaving attack. Defense against Gray Hole Attack: In [15] author described a Feasible Solution for detection and removal of gray hole attack. Each point can locally maintain its own table of black listed points whenever it tries to send data to any destination point and that point can also aware the network about the black listed points. This list of malicious point scan be applied to discover secure path from source to destination by avoiding multiple grey hole points acting in corporation.

D. Flooding Attack: As with traditional networks, the hazard of a flooding aggression applies. Such an aggression is tough to distinguish from a sudden but legitimate increase in network traffic [8]. A malicious point could endeavor to flood the network with its own unjust data packets, potentially using many different destination addresses. Gupta, Krishnamurthy and Faloutsos show how two connive points, at adverse ends of a network; can segregation the network by sending a huge volume of data between them. While the authors concentrate on occupying the wireless medium by exploiting the vulnerabilities of IEEE 802.11, the attack also causes denial of service by debilitating the intermediate points which forward the high volume of traffic generated.

Thus, one aggression can simultaneously achieve more than one type of rebuttal of service. A related but more localized aggression arises when a malicious point sends its neighbours packets to forward at a rate at which the neighbours become overwhelmed. The pacing protocol is a mechanism used by the DARPA Packet Radio Network (PRNET) [18, 20], in which points measure the ahead lag of their neighbours in order to pace the rate at which to send packets to their neighbours for aheading. Thus, a malicious point could deliberately not follow the pacing protocol and encompass its neighbours with packets. Gupta, Krishnamurthy and Faloutsos [20] define the effects of such an attack on the link layer.

Maliciously sending a huge volume of packets not only prevents immediate neighbours from accessing the wireless medium, but also deprives points in the 2-hop neighbourhood of the suspected point of network connectivity. This exploits the 'capture effect', whereby a point with a bulky traffic load will grab the wireless medium and avert a point with a lighter traffic load from penetrating the medium. When using routing protocols which can all togetherroute data forward multiple ways, a flooding attack can disturb an even greater capacity of the network. Finally, note that the payload of each packet does not necessarily have to contain any useful information; the attacker only has to assure that the packet headers contain the right information.

E. Jellyfish Attack: In jellyfish attack the malicious point first intrudes into the forwarding group in the network and then it unreasonably lags data packets for some amount of time before forwarding them. This result in no doubt high end to- end delay and delay jitter, and thus demean the achievement of real-time applications.

F. Modification Attack: Modification attacks associate meddles with our asset. Such attacks might primarily be advised an integrity attack but could also produce an availability attack. If we approach a file in an unauthorized way and alter the data it contains, we have afflicted the integrity of the data enclose in the file. Nonetheless, if we consider the case where the file in question is a configuration file that administers how a distinct service act, May be one that is acting as a Web server, we potency influence the availability of that service by changing the texts of the file. If we extend with this match and say the configuration we modified in the file for our Web server is one that modifies how the server deals with encrypted connections, we keep alike make this a confidentiality attack.

G. Impersonation Attack: In Ad-Hoc networks a point is free to move in and out of the network. There is no secure authentication process in order to make the network secure from malicious points. In MANETs IP and MAC address uniquely identifies the host. These measurements are not abundantly to authenticate sender. The attacker avail MAC and IP spoofing in order to obtain identity of someone else point and shelter into the network. This type of attack is also known as spoofing attack [13]. Aegis against Impersonation Attack: As it may be used to contend against impersonation as well as repudiation attacks. ARAN affords authentication and non-repudiation services using prearranged cryptographic certificates for end-to-end authentication. In ARAN, individual point requests a certificate from a trusted certificate server. Route analysis is accomplished by broadcasting a route discovery message RDP from the source node. The reply message REP is unicast from the destination to the origin. The routing messages are authenticated at each intermediate hop in both directions.

III. SECURE ROUTING TECHNIQUES

A. Watchdog and Pathrater: Watchdog and Pathrater are two main components of a system that tries to improve performance of ad hoc networks in the presence of malicious points [12,13]. Watchdog determines misbehavior by copying packets to be forwarded into a buffer and monitoring the behavior of the adjacent point to these packets. Watchdog promiscuously snoops to decide if the adjacent point forwards the packets without modifications in it or not. If the packets that are snooped match with the observing point's buffer, then these packets are discarded; whereas packets that stay in the buffer apart from a timeout period beyond any successful match are flagged as having been discarded or modified. The point responsible for forwarding the packet is then noted as being selective. If the number of violations becomes higher than a certain predetermined threshold, the violating point is marked as being malicious. Information about malicious points is passed to the Path rater component for inclusion in path rating evaluation. Path rater on an individual point works to rate all of the known points in a particular network with respect to their reliabilities. Ratings are made, and updated, from a particular point's per spectate. Points start with a neutral rating that is modified over time based on observed reliable or unreliable behavior during packet routing. Points that are observed by watchdog as malicious has given an immediate rating of -100. It should be dignified that misbehavior is disclosed as packet mishandling/modification, whereas unreliable behavior is disclosed as link breaks. It is shown from the experiments that these two components can well reflect the reliability of the points based on their packet forwarding performances.

IV.CONCLUSION

In this analysis paper, Authors try to check out the security risk in mobile ad hoc networks, which may be a main brawl to the operation of it. It shows little typical &dangerous vulnerability in MANET. It further presents the crucial attack types that threaten the current MANET, their aegis mechanism &several security approaches that can conserve the MANET from attacks. Analyze on MANET is still in an early phase. Actual proposals are typically based on one clear-cut attack. They could work fine in the presence of designated attacks, but there are many unanticipated or combined attacks that hover undiscovered. A lot of research is allaying on the way to analyze new threats and create secure mechanisms to resist those threats. More research can be done on integrated approaches to routing security and data security at distinct layers.

V. REFERENCES

[1]. M. Parsons and P.Ebinger, "Performance Evaluation of the Impact of Attacks on mobile Ad-Hocnetworks. https://pdfs.semanticscholar.org/6a87/fbd85d704e2de14e8738f6d5ff075a8fca9f.pdf

[2]. P.V.Jani, "Security within Ad-Hoc Networks," Position Paper, PAMPAS Workshop, Sept. 16/17 2002.

[3]. G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for performance Improvement in MANET", Karlstads University, Sweden, December 2006

[4]. S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.

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

[6]. 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.

[7]. N.Shanti, Lganesan and K.Ramar, "Study of Different Attacks On Multicast Mobile Ad-HocNetwork". 8C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile AdHoc Networks", Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[8]. Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacksin Wireless Ad Hoc Networks, in Proceedings of IEEE INFOCOM'03, 2003.

[9]. Y. Hu, A. Perrig and D. Johnson, Wormhole Attacks in Wireless Networks, IEEEJournal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.

[10]. Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad HocNetwork Routing Protocols, in Proceedings of ACM MobiCom Workshop - WiSe'03,2003.

[11]. Sergio Marti, T. J. Giuli, Kevin Lai and Mary Baker, Mitigating routing misbehavior inmobile ad hoc networks, in Proceedings of the 6th annual international conference on Mobilecomputing and networking (MobiCom'00),pages 255–265, Boston, MA, 2000.

[12]. Jim Parker, Discussion Record for the 1st MANET Reading Group Meeting,http://logos.cs.umbc.edu/wiki/eb/index.php/February_10%2C_2006 (Authorizationrequired).

[13]. Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks - A Survey".

[14]. Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[15]. A Study of wireless Ad-Hoc Network attack and Routing Protocol attack M Kumar, A Bhushan, A Kumar International Journal of Advanced Research in Computer Science 2, 4

[16]. FahadSamad, Qassen Abu Ahmed, AsadullahShaikh and Abdul Aziz, "JAM: Mitigating Jellyfish Attack in Wireless Ad hoc Networks",B.S. Chowdhary et.al.(Eds.):IMTIC 2012,CCIS 281,PP, 432-144.2012.

[17]. 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.

[18]. 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.

[19]. S.Marti, T.J.Giuli, K.Lai, M.Baker, "Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks".

[20]. Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks. Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), pp. 3-13,2002.

[21]. K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEE -E International Conference on Network Protocols (ICNP), pp. 78-87, 2002

Cite this article as :

Pawitar Dulari, "A Study of Attack on Wireless Ad-Hoc Network", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 6, pp. 168-174, November-December 2019. Available at doi : https://doi.org/10.32628/IJSRSET196646
Journal URL : http://ijsrset.com/IJSRSET196646