International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.6, No.11, November 2017 DOI:10.15693/ijaist/2017.v6i11.30-36

Attack prediction and detection in Ad-hoc Wireless sensor network-A review

[1]M. Dhanabhagyam, [2]M.Devapriya
[1]Research Scholar, [2]Assistant Professor,
[1, 2,] Department of Computer Science
[1, 2,] Government Arts College (Autonomous) Coimbatore-18, Tamil Nadu

Abstract

In recent days, networking plays a major role in communication with several attributes. In network security is the main objective that decides the quality of service. Several researchers focused more on ad hoc networks and its routing. In traditional research some limitations are identified by the researchers that are localization, attack free network maintenance and enhanced lifetime. In sensor network, the error free and fault free transmission is needed to provide good accuracy and efficiency. Therefore, this research analysed several traditional methodologies and algorithms to maintain the error free routing. Some techniques covered in this survey are tabulated with its merits and demerits. Finally, the problem is identified in routing section with several number of attacks. Particularly, the review is separated into detection of attacks, determining the attackers in a multiple adversaries and localizing multiple adversary attackers. Furthermore, the research suggested to improve the routing performance by completely detecting the attacks.

Keywords--- Ad hoc networks, Security, Attacks, Side-channel attacks, Lifetime improvement

I. INTRODUCTION

The wireless sensor networks are deployed around the environment with attractive targets. Normally, the sensor network is open that may cause more vulnerable to attacks. The attacks results in serious treats and corrupt the data transmission and reception. Hence, it is necessary to detect, maintain and eliminate the attacks. Several number of researchers concentrated more on securing the data between sensing unit and base station. Moreover, the attack detection is defined as to find the unauthorized access by the outsiders. The attack prediction is stated as to find the misuse location or path which is created by bypassing the route and find the misuse state in a network. Network security always begins with a username and a secret key for authorization. The system security comprises of several arrangements and approaches that are received by a system executive to avoid and monitor unapproved access, alteration in framework, abuse, or denial of network available assets. Essentially, the network security includes the approval of access to the information in a network, which is controlled by the network administrator. It has turned out to be more imperative to clients and associations.

To overcome such issues, a firewall powers to get the arrangements for organizing clients. So that to prevent unapproved access to framework, this segment may neglect to check conceivably hurtful substance or Trojans being transmitted over the system. Anti-infection programming or an Intrusion Detection System (IDS) helps to recognize the malware. Today abnormality may likewise screen the system like wire shark movement and might be logged for review purposes and for later on abnormal state investigation in system. Communication between two hosts utilizing a system might be utilizes encryption to keep up protection approach.

Every hub in the system acts as a router and transfers the information packets to different hubs. Because of hub movement, topology of the system is always fluctuating gradually which execute the considerable difficulties to the security of Mobile Ad Hoc Network. Accordingly, assailant can get advantages of imperfection in routing protocols to complete an assortment of attacks. Some attacks aggravate the routing protocol and harms the system's topology. The general form of attacks is classified into different types. Figure 1.1 shows the attack types. Passive attacks are those where the assailant does not irritate the operation of the routing convention, endeavour’s to look for some significant data through

Activity examination. This thus can prompt the divulgence of basic data about the system or hubs, for example, the system topology, the area of hubs or the personality of essential hubs.

Generally, the outsider attacks are defined as the attack that does not belong to a WSN node. Insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways. The types of active attacks are spoofing, Wormhole, Modification, Denial of services, Sinkhole, and Sybil attack. If a node is in out of identity, then the sender change its topology, it is called as spoofing. Similar to that, if the Malicious node results in some modification in one Route, so that there is a need for taking long route and named it as modification. Hence, more delay gets occurred. Another attack is named as wormhole or tunnelling attack, it is because of the attacker receives a packet at one point and underpasses it to another affected node. By misunderstanding, the sender thinks that tunnelling is a shortest path. The Fabrication attack is one of the attack created by means of false routing message which is generated by the harm node. Hence, it is states incorrect information about the route between devices.

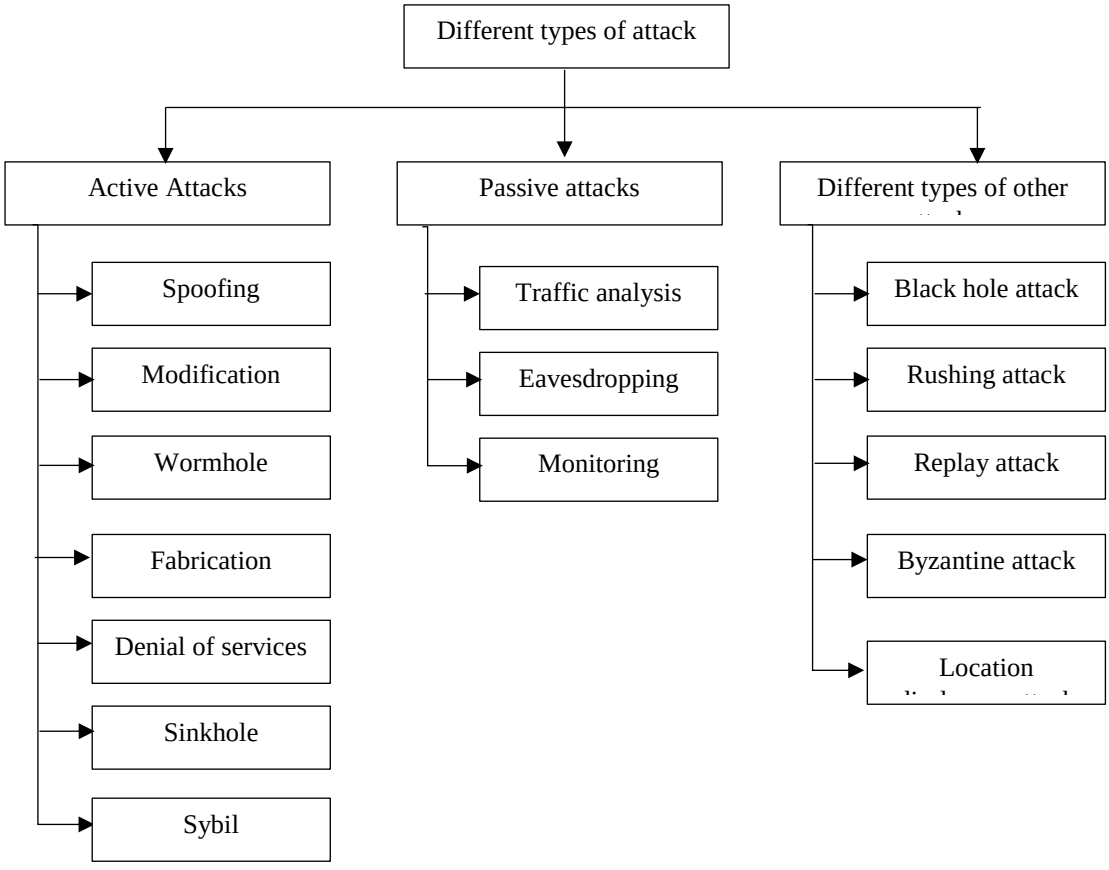

Figure 1.1 Classification of attacks

Similar to active attacks, some passive attacks are represented here to manage the traffic analysis. The normal traffic analysis is depends on the communication path between source and destination. Hence, it is easy to find communication path by attacker without any modification. Eavesdropping is one of the passive attack utilized for detecting the confidential information. Example: Public key or Private Key. Finally, the monitoring is also one of the Attack that scan confidential data without any editing option. The main contribution of this research is to analyse various factors such as types of attacks. Section 2 discuses about the recent attack types with its merits and demerits in ad-hoc networks. Finally, the problem is identified and stated in section 3. It helps to implement future directions and decide the detection process.

II. LITERATURE SURVEY

This section discusses in detail about various attacks that are involved in wireless ad-hoc networks with numerous mechanism concentrated by various dramatists. Security parameters in WSN are now receiving popularity in the investigation. In recent days, different real time ad-hoc applications occupies large areas like military and other medical fields. Based on the applications, the programming nature, utilizing field and other characteristic is varied. Given their attractive normal for quick and simple organization, MANETs are considered as a perfect network for building up the proper communication networks and frame the administrations by means of natural disasters, earth quakes and surges.

Table 1.1 Comparison of traditional methods

Sl.No	Author	Method used	Attack Considered	Discussion
1	Patcha, A., & Mishra, A. (2003)	Router: AODV Protocol Simulator: NS-2.32 Simulation Time: 900 sec No of Nodes: 50	Black hole attack	To analyse the node in unstable operations. It reviewed Malicious nodes detection and colluding. Here only fixed number of nodes are analysed. They suggested to handle more experiments on movable nodes.
2	Park, S., Aslam, B., Turgut, D., & Zou, C. C. (2009)	In road side units of VANET	Sybil Attack	Complex roadways are considered here for analysing the traffic. Need to analysed different it for various traffic situations Example: Traffic congestion
3	Cai, J., Yi, P., Chen, J., Wang, Z., & Liu, N. (2010)	Path-based method and adaptive algorithm	Black and Gray Hole Attacks	Adaptive Approach is considered to Detect these two attacks. Need to improve the detection rate and avoid the attack rate.
4	Arya, M., & Jain, Y. K. (2011).	Router: AODV, Gray Hole AODV, IDSAODV Simulation Time: 100 ms Mobile nodes: 7, 20	Gray hole Attack	Routing, Packet Delivery ration and throughput is analysed. In future, it is required to enhance the detection in each and every misbehaviour detection and transmission rate of metrics compare with the all Protocols
5	Gandhewar, N., & Patel (2012)	Router: AODV Protocol Simulator: NS-2.32 Simulation Time: 500 sec No of Nodes: 10-50	Sinkhole Attack	It considered AODV protocol for analysing. To consider different routing protocol and find the detection and evaluate the performance.
6	Pal, A. (2013).	DSR Neighbouring nodes' RREQs packets	Sleep deprivation	Mechanism to protect against sleep deprivation through traffic injection
7	Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015).	Routing: Dynamic source routing (DSR), Best-Effort Fault-Tolerant Routing (BFTR)	Collaborative Attacks by Malicious Nodes	It compares cooperative bait detection scheme and DSR schemes. There is a need for comprehensive secure routing framework to protect MANETs against miscreants.
8	Li, W., & Song, H. (2016).	An Attack-Resistant Trust Management Scheme in VANET	Malicious attacks	Attack-Resistant Trust management scheme (ART) is proposed to detect the attack. Need to increase the precision rate

Another significant utilization of MANETs is on-the-fly collective registering outside an office domain, in a group venture offsite, or amid an offsite meeting. Scientists are likewise exploring the details of utilization situations for MANETs in business areas. Some traditional methods utilized for detecting the attacks are mentioned in table 1.1 with its routing structure.

Some recent research are identified and reviewed based on its applications. Likewise, Jhaveri et al., (2012) reviewed Denial-of-Service (DoS) attacks namely Wormhole attack, Black hole attack and Gray whole attack. As MANETs are generally utilized as a part of numerous indispensable applications, bunches of research work must be done to discover effective arrangements against these DoS assaults that can work for various directing conventions. Similar to that, Vampire attacks is one of the complex attack, it is analysed by Vasserman and Hopper (2013).

Loo et al., (2016) framed a recent trends in mobile ad-hoc networks. As of now, a few research determinations were propelled to counter against these pernicious attacks. A large portion of the past work focused most of the part on giving preventive plans to ensure the directing convention in a MANET. The vast majority of these plans depend on key administration or encryption procedures to prevent unapproved hubs from joining the system. The major limitations of the traditional methods is that they introduce a huge traffic load to interchange the key lines. Another major drawback is very expensive and its speed need to be improved.

Marti et al., (2000) presented the models to identify the Colluding Misrelay Attack and improve the overall efficiency of the packet routing. Normally, this attack is very difficult to recognize in traditional methods such as watchdog and pathrater. Colluding miserly attack occurs in a routing path especially in proactive MANET networks. It is because of the directing packets bound to all hubs in the system that requires all hubs to restore an ACK, this could prompt a huge overhead, which is thought to be inefficient. Karakehayov, Z. (2005) presented a method to detect this attack with multiple malicious nodes. It represents the colluding of two packets framed by the attackers. It requires additional power to detect the attack and major limitations are it may not detect the attack if it has more than three attacks. Finally, the suggestion is framed as the fundamental downside of this approach is that regardless of the possibility that we require every hub to build transmission energy to be K times, despite everything we can't recognize the assault in which K + 1 attackers work in agreement to drop packets. Along these lines, additionally work must be done to counter against this sort of attack productively.

Clausen, D. R. C. A. T., & Mühlethaler, P. (2005) presented the protection logic against wormhole attack in the OLSR protocol. It is framed by means of detecting the location information and public key source from all nodes which is similar to the Hu et al., (2006) proposed logic. The working principle of this method is to find the length of the source node to the destination node. If it results in maximum distance then it is predicated as warm whole attack.

Distributed Denial of Service (DDoS) attacks are a virulent, relatively new type of attack on the availability of Internet services and resources. DDoS attackers infiltrate large numbers of computers by exploiting software vulnerabilities, to set up DDoS attack networks. These unwitting computers are then invoked to wage a coordinated, large-scale attack against one or more victim systems. As specific countermeasures are developed, attackers enhance existing DDoS attack tools, developing new and derivative DDoS techniques and attack tools. Rather than react to new attacks with specific countermeasures, it would be desirable to develop comprehensive DDoS solutions that defend against known and future DDoS attack variants. However, this requires a comprehensive understanding of the scope and techniques used in different DDoS attacks.

A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource. A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. The services under attack are those of the “primary victim”, while the compromised systems used to launch the attack are often called the “secondary victims.” Desilva, S., & Boppana, R. V. (2005) proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect

malicious RREQ floods and avoid the forwarding of such packets.

Flooding Attack is rectified by Yi et al., (2005), with a simple mechanism in the AODV protocol. In this approach, each node monitors and calculates the rate of its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. The drawback of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. In another case, if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake, it is one of the serious issue.

Al-Shurman et al., (2004) proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

Kurosawa et al., (2007) analysed the blackhole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. Based on this analysis, the authors propose a statistical based anomaly detection approach to detect the blackhole attack, based on differences between the destination sequence numbers of the received RREPs.

III. Conclusion

A MANET is a rising innovation that has been pulling in enormous consideration from specialists. Since these systems can be conveyed rapidly without depending on a predefined framework, they can be connected in different circumstances running from crisis operations and disaster relief to military administration and teams. Clearly, giving security in such situations is basic. The fundamental shortcomings of a MANET are that it is asset obliged, for instance, a MANET has restricted data transfer capacity, battery control, and computational power, and it does not have a dependable concentrated organization. Hence, existing security plans for wire systems can't be connected straightforwardly to a MANET, which makes a MANET significantly more vulnerable against security attacks.

In this survey, it is noticed that the current state of- the-art of routing attacks in an ad-hoc networks. For precautions, we identified their advantages as well as their drawbacks. Our studies showed that although many solutions have been proposed, they still are not perfect in terms of trade-offs between effectiveness and efficiency. For example, some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource-constrained MANETs.

The future suggestions of this work are

i. Implement the detection module to detect the presence of attacks even in multiple colluding attackers.
ii. It is necessary to detect and monitor the active attacks like Modification, worm hole and fabrication.
iii. Eliminate the delay and improve the network lifetime to maximize the overall performance.

References

[1]. Gandhewar, N., & Patel, R. (2012, November). Detection and Prevention of sinkhole attack on AODV Protocol in Mobile Adhoc Network. In *Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on* (pp. 714-718). IEEE.

[2]. Patcha, A., & Mishra, A. (2003, August). Collaborative security architecture for black hole attack prevention in mobile ad hoc networks. In *Radio and Wireless Conference, 2003. RAWCON'03. Proceedings* (pp. 75-78). IEEE.

[3]. Arya, M., & Jain, Y. K. (2011). Grayhole attack and prevention in mobile adhoc network. *International Journal of Computer Applications*, *27*(10).

[4]. Park, S., Aslam, B., Turgut, D., & Zou, C. C. (2009, October). Defense against sybil attack in vehicular ad hoc network based on

[5]. roadside unit support. In *Military Communications Conference, 2009. MILCOM 2009. IEEE* (pp. 1-7). IEEE.

[6]. Cai, J., Yi, P., Chen, J., Wang, Z., & Liu, N. (2010, April). An adaptive approach to detecting black and gray hole attacks in ad hoc network. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on* (pp. 775-780). IEEE.

[7]. Li, W., & Song, H. (2016). ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, *17*(4), 960-969.

[8]. Chang, J. M., Tsou, P. C., Woungang, I., Chao, H. C., & Lai, C. F. (2015). Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach. *IEEE systems journal*, *9*(1), 65-75.

[9]. Pal, A. (2013). *Dynamic routing with cross-layer adaptations for multi-hop wireless networks* (Doctoral dissertation, The University of North Carolina at Charlotte).

[10]. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). DoS attacks in mobile ad hoc networks: A survey. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* (pp. 535-541). IEEE

[11]. Vasserman, E. Y., & Hopper, N. (2013). Vampire attacks: draining life from wireless ad hoc sensor networks. *IEEE transactions on mobile computing*, *12*(2), 318-332.

[12]. Loo, J., Mauri, J. L., & Ortiz, J. H. (Eds.). (2016). *Mobile ad hoc networks: current status and future trends*. CRC Press.

[13]. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 255-265). ACM.

[14]. Karakehayov, Z. (2005). Using REWARD to detect team black-hole attacks in wireless sensor networks. *Wksp. Real-World Wireless Sensor Networks*, 20-21

[15]. Clausen, D. R. C. A. T., & Mühlethaler, P. (2005). Securing OLSR Using Node Locations. *Proc. 2005 Euro. Wireless, Nicosia, Cyprus*.

[16]. Hu, Y. C., Perrig, A., & Johnson, D. B. (2006). Wormhole attacks in wireless networks. *IEEE journal on selected areas in communications*, *24*(2), 370-380

[17]. Desilva, S., & Boppana, R. V. (2005, March). Mitigating malicious control packet floods in ad hoc networks. In *Wireless Communications and Networking Conference, 2005 IEEE* (Vol. 4, pp. 2112-2117). IEEE

[18]. Yi, P., Dai, Z., Zhang, S., & Zhong, Y. (2005). A new routing attack in mobile ad hoc networks. *International Journal of Information Technology*, *11*(2), 83-94.

[19]. Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In *Proceedings of the 42nd annual Southeast regional conference* (pp. 96-97). ACM.

[20]. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., & Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *IJ Network Security*, *5*(3), 338-346.

[21]. Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). A novel approach for grayhole and blackhole attacks in mobile ad hoc networks. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*(pp. 556-560). IEEE.

Author Profile

Dr. M.Devapriya received her M.Sc., Computer Science from PSG College of Arts and Science Coimbatore in the year 1991. She obtained her M.Phil. And Ph.D., degree from Mother Teresa Women's University, Kodaikanal in the year 2001 and 2011 respectively. She is having around 18 years of teaching experience in various colleges. At present she is working as an Assistant Professor of Computer Science, Government Arts College, Coimbatore. She has published more than 15 papers in National, International journals and Conferences. Her area of interest includes

Object Oriented Programming, Image Processing, Multimedia Security and Computer Networks. She is a member of various professional bodies.

M. Dhanabhagyam, received the B.Sc. degree in Computer Science in 2011, from kovai kalaimagal college of Arts & Science, Coimbatore India and M.Sc. degree in computer Sciences in 2014 from Government Arts College (BU), Coimbatore, India. And B.Sc.Btd degree in Computer Science in 2015 from st's Mark College of Education, Coimbatore India. And now she is Mphil Research Scholer in Government Arts College (Autonomous) Coimbatore, India. His area of interests networking.