Intrusion Detection System for Wireless Networks: A Review

[1]Vikas Singla, [2]Monika Sachdeva and [3]Sunil Kumar Gupta
[1]Punjab Technical University, Jalandhar
[2]Shaheed Bhagat Singh State Technical Campus, Ferozpur
[3]Beant College of Engineering & Technology, Gurdaspur
E-mail: [1]singla_vikas123@yahoo.com, [2]monika.sal@rediffmail.com, [3]skgbcetgsp@gmail.com

***Abstract*—Wireless networks have recently been gaining widespread deployment and they can be easily attacked as compared to wired networks. CERT statistics reports state that the amount of intrusions on network has excessively increased year by year. With the increasing amount of network throughput and security threat, the study of intrusion detection systems (IDSs) has received a lot of attention throughout the computer science field. The traditional wired IDS is a great system, but unfortunately it does little for the wireless world. In this paper we will do the comprehensive survey and review the current security techniques and some IDS systems for protection against various types of attacks in wireless networks.**

Keywords: Wireless Network, Intrusion Detection, Attacks, Security

I. Introduction

In today's arena, Wireless Networks are more popular and better alternative as compared to wired networks. In today's life, we will find wireless networks everywhere e.g. at homes, an offices, or at business places. The development of wireless networks offers the promise of a flexible, low cost solution for monitoring critical infrastructure. The biggest concern with wireless network has been security. Security methods are designed in order to avoid unauthorized access to system assets and information. Be that as it may, totally avoiding breaks of security, at present, doubtful. However, We can attempt to identify these Intrusion endeavors. This field of research is known as Intrusion Detection. Intrusion detection system is method which secure our network from various kind of attacks [1, 4]. The main purpose of intruder is to hack the important information in the network, like using the bandwidth of node or increasing the delay time in providing the services over the network under consideration.

Other Sections in the paper are structured as follows. Section 2 of the paper defines the various security goals. Section 3 gives classification of different attacks on wireless network. Section 4 presents the Literature Review. Finally, we are concluding the paper with some goals for future work.

II. Security Goals

Any routing protocol must have an essential set of security mechanisms. These type of mechanisms help to prevent, detect, and respond to different types of security attacks [6]. Different types of security goals are required to be dealt with for maintaining a reliable and secure ad-hoc network. These are as below:

1. *Authentication*: This is concerned with unintended users are not be authorized to enter into the network. Authentication is assurance that the user tries to enter into the network is authentic user what it is claiming and it is not the intruder. An attacker tries to impersonate the user and thus getting unauthorized access to network and sensitive information of the network. Authentication is not to allow such types of users to access the network.
2. *Confidentiality*: Protection of any information from being exposed to unintended users. This is concerned with sending the message in such a way that unintended users cannot read the actual contents of the message. In ad-hoc networks confidentiality is more difficult to achieve as in the ad-hoc networks intermediates nodes receive the packets from other recipients.
3. *Availability:* Services are required to be provided when required. Availability is basically concerns with the availability of network. It has no concern with the actual data sent over the network. On the physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol.
4. *Integrity*: Message being transmitted is never altered. Data integrity has more importance than confidentiality. The reason is that by means of confidentiality, the attacker is only able to see the physical environment. And by means of reading the data, they are only able to read where the sensors are actually placed..But if the attacker is successful in alteration of data, the deployer of wireless sensor network will not be able to know what is actually happening in the network.

III. Classification of Attacks

Due to their underlined architecture, wireless networks are more easily attacked than a wired network. The attacks on wireless routing protocols can be broadly classified into following categories [4, 5, 6].

1. *Passive Attacks*, has no concern with the operation of the protocol. Passive attacks try to find the useful information about the network. Suck kind of attacks tries to collect the routing information

by sniffing the network. Passive attacks are difficult to detect. Due to this providing security against passive attacks is more complex. Using passive attacks, attacker can identify the network topology, however using these attacks it is difficult to find the actual location of node.

2. *Active Attacks*, the main function of these type of attacks is to disrupt the operation of the protocol by inserting arbitrary packets into the network. This kind of attacks tries to get authentication into the network so that they can access all the packets travelling over the network and disabling the operation of network.
3. *Denial-of-Service attacks (DoS)*, cause a network to slow down or become unusable. In case of DoS attack, attacker generates traffic, insert this into the network, which in turn block the server for a long. Distributed Denial-of-Service attacks (DDoS) occurs when many computers are used against the target.
4. *Man-in-the-middle attack*, will occur when the attacker is able to read and edit the communications between the two parties without the parties are being aware of the presence of attacker.

IV. Literature Review

The various solutions provided by different authors from above said attacks by providing some intrusion detection system are discussed below.

Madhavi *et al.* [8] inspect the vulnerabilities of wireless network and contended that intrusion detection must be incorporated in the security system. They proposed a Mobile Intrusion Detection System suitable for wireless networks, which distinguishes nodes misbehavior, irregularities in packet sending, for example, some nodes dropping packets. Proposed System does depend on overhearing packet transmissions of neighboring nodes. Proposed System sets the various thresholds dynamically.

Biradar *et al.* [10] proposed a security based multicast routing mechanism in MANET. Proposed method finds multicast routes to receivers by calculating route request packets and route reply packets. Performance of the proposed method is compared with on-demand multicast routing protocol and enhanced on-demand multicast routing protocol. They presumed that the proposed method delivers better PDF, reduced packet delay and reduced overheads.

Bhatnagar *et al.* [11] examined about issues and difficulties of IDS system for wireless sensor network and suggested a secure method that can recognize possible intrusion in the network, alarming client after intrusion had been discovered and reconfigure the system. In this paper, authors are mainly focused in multi hop WSNs and proposed an intrusion detection system using decision making technique.

Table 1 Literature Survey

Author	Publication Year	Proposed IDS Scheme/ Technology	Work Done	Conclusion
Madhavi *et al.,* [8]	2008	Mobile Intrusion Detection System	Propose an MIDS Suitable for Multi-Hop Ad-Hoc Wireless Networks, Which Find Out Misbehavior Nodes and Packet Forwarding Anomalies.	They Proposed MIDS Which Detects Packet Drops or Delays that Violate the Respective Flow Requirements.
Biradar *et al.* [10]	2010	A stability based multicast routing scheme	Performance of the method suggested by them is compared with ODMRP protocol (on-demand multicast routing protocol) and EODMRP protocol (enhanced on-demand multicast routing protocol).	Method suggested by them provided good PDR (packet delivery ratio), less packet delay and less overheads.
Bhatnagar *et al.* [11]	2010	Decision Making Technique	Discussed about various challenges in intrusion detection system for wireless network and proposed a new method for securing the network.	Proposed intrusion detection system defenses the strength of a wireless sensor networks using decision making technique.
Ming-Yang Su [12]	2011	Anti-Blackhole Mechanism	Detect and separate malicious nodes.	When the suspicious value exceeds the threshold value, an IDS nearby will send a broadcast message to all nodes saying them to cooperatively isolate the malicious node.
Sharma *et al.* [13]	2011	Misuse Detection System	Proposed a new Network Intrusion System that detects the Denial of Service(DoS) attack of Wireless Network.	The proposed method provided the safer transmission in Denial of Service and Man in Middle Attack.
Mulert *et al.* [14]	2012	Reactive intrusion detection node blacklisting scheme.	Analysis of SAODV to identify unresolved threats to the algorithm, such as medium access control layer misbehavior, resources depletion, black holes, worm- holes, jellyfish and rushing attacks.	Provide solution to various threats in MANET using AODV and SAODV

Ming-Yang Su [12] provided a mechanism for finding and separating the malicious nodes in the network. All IDS nodes perform a mechanism known as Anti-Black-hole mechanism, which assesses the suspicious estimation of a node by calculating difference between RREPs and RREQs transmitted over the node. At the point when a suspicious value exceeds the threshold value, an IDS adjacent will broadcast a block message, advising all nodes on the system, requesting them to helpfully disconnect the malicious node.

Sharma *et al.* [13] proposed an Network Intrusion System that will detect the Denial of Service Attack. The proposed method will finds the intrusion, on the bases of the Misuse Detection which has less false negative. Proposed System detects the intruders by the IP address.

Muler *et al.* [14] worked on networks using AODV and Secure AODV Protocols. They conducted a vulnerability analysis of SAODV to recognize uncertain threats to the algorithm, for example, medium access control layer misconduct, assets consumption, black holes etc. They contrast this helplessness investigation and proposed method to handle the distinguished attacks. They proposed method that incorporate multipath routing, incentive schemes, directional antennae, packet leashes etc.

V. Conclusion and Future Scope

In this paper, we present a review of recent work on different approaches of Intrusion detection system for wireless networks. Each technique has its own superiority and limitations, so that we should be cautious about selecting the technique. We provide a table which summarized the work of different authors to easily grasp the overall picture. We provide a comprehensive review of IDSs. However, there remain many open issues and future challenges.

Acknowledgment

Authors wish to thank Punjab Technical University, Jalandhar for providing inspiring environment for research work.

References

[1] Cabrera, J.B.D., Ravichandran, B & Mehra R.K., "Statistical Traffic Modelling for Network Intrusion Detection", In Proceeding of the IEEE Conference (2000).

[2] Y. Zhang, W. Lee., "Intrusion detection in wireless ad-hoc networks", In Mobile Computing and Networking, (2000), pp. 275–283.

[3] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe and K. Levitt, "A specification-based intrusion detection system for AODV." In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, (2003), pp. 125–134.

[4] W. Zhang, R. Rao, G. Cao and G. Kesidis, "Secure routing in ad hoc networks and a related intrusion detection problem." In Proceedings of the IEEE Military Communications Conference, (2003), pp. 735–740.

[5] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion Detection in Wireless Ad-Hoc Networks." In IEEE Wireless Communications, (2004), pp. 48–60.

[6] A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks", In Communications of the ACM, Vol. 47, No. 6, (2004), pp. 53–57.

[7] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, Yoshiaki, Nemoto, "Detecting black hole attack on AODV-based Mobile Ad Hoc Networks by dynamic learning method", International Journal of Network Security 5 (2007), pp. 338–346.

[8] S. Madhavi, Tai Hoon Kim,"An Intrusion detection system in mobile adhoc networks", International Journal of Security and Its Applications, Vol. 2, No. 3, (2008) pp. 1–16.

[9] R. Huang, Y. Zhuang, Q. Cao, "Simulation and Analysis of Protocols in Ad Hoc Network", International Conference on Electronic Computer Technology IEEE (2009).

[10] R. Biradar, S. Manvi, M. Reddy, "Link stability based multicast routing scheme in MANET", Computer Networks 54 of Elsevier (2010), pp. 1183–1196.

[11] R. Bhatnagar, A.K. Srivastava, A. Sharma, " An Implementation Approach for Intrusion Detection System in Wireless sensor Network", International Journal on Computer Science and Engineering Vol. 02, No. 07, (2010), pp. 2453–2456.

[12] M.Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications 34 (2011) pp. 107–117.

[13] M. Sharma, Anuradha, " Network Intrusion Detection System for Denial of Service Attack based on Misuse Detection", International Journal of Computational Engineering & Management Vol. 12, (2011) ISSN (Online): 2230–7893, pp. 19–23.

[14] J.V. Mulert, I. Welch, W.K.G Seah, "Security threats and solutions in MANETs: A case study using AODV and SAODV", A Journal of Network and Computer Applications 35 (2012) of Elsevier, pp. 1249–1259.