ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

Intrusion Detection System Survey for Mobile Ad-Hoc Networks

Ms. Priyanshi Jaiswal[1], Prof. Amit Kumar Sariya[2]

Alpine Institute of Technology, Ujjain[1,2]

Abstract: Mobile ad-hoc network needs to take major concern of security due to vulnerable open environment and non-stationary mode. Mostly, offenders focus to attack on victim using these venerable points to affect resources and performance of the networks. Kinds of attack targeted on victim nodes which are influence resources actively and passively. Several works have been done to detect and mitigate such kind of attacks, but still some more work required. In this paper, different activity of intrusion and IDS Schemes are discussed.

Keywords: Mobile Ad-hoc Networks, IDS, Watchdog, Pathrater, AACK

I. INTRODUCTION

In ad-hoc network each node has facility to move anywhere in network area without co-ordination, thus mobility of nodes make network vulnerable in security aspect. Security is one of the most important constraints for the ad hoc network performance. This vulnerability invite attacker to attacking several kinds of attacks on the network resources. These attacks impact on network throughput, performance and lifetime. A lot of research have been done against attacks and required more research to defend the network resources from different attacks by detecting and preventing data from detected attack. Efforts are putting to improve the network security mechanism for smooth network operations against intrusion.

A. Application Domain

- **Collaborative Work:** For some business environments, the need for collaborative computing might be more important outside office environments than inside [1]. After all, it is often the case where people do need to have outside meetings to cooperate and exchange information on a given project.
- **Crisis-management Applications:** these arise, for example, as a result of natural disasters where the entire communications infrastructure is in disorder. Restoring communications quickly is essential. By using ad hoc networks, a communication channel could be set up in hours instead of days/weeks required for wire-line communications.
- **Personal Area Networking and Bluetooth:** a personal area network (PAN) is a short- range, localized network where nodes are usually associated with a given person [2]. These nodes could be attached to someone's pulse watch, belt, and so on. In these scenarios, mobility is only a major consideration when interaction among several PANs is necessary.

II. LITERATURE SURVEY

During the last few years various authors have published so many documents to carry forward the wormhole detection work. According to most of them the work can be done effectively by taking multiple environmental factors to get the accurate analysis & design of methodologies. Some of them is given as follows:

Marti et al. [3] proposed Watchdog technique as well as Pathrater techniques in 2000 that improve network performance within presence of misbehaving nodes. Watchdog uses to detect misbehaving nodes in a network that agree to forward packets but fail to do so, while Pathrater technique uses to avoid these misbehaving nodes in a route path in the future transmission. The integrating of Watchdog and Pathrater techniques improve network performance significantly [3] in MANETs. Watchdog technique detects the misbehaving nodes by applying promiscuous mode, where each node listens to its neighbor transmissions. If the next node in a route path fails to forward the sent packet, It increases its failure counter. Then it determines the node as misbehaving if the failure counter exceeds a certain predefine threshold. As a result, the Pathrater technique avoids this node in the future transmission by cooperating with routing protocol to choose different path from source to destination depending on the used algorithm. Even though Watchdog and Pathrater techniques are able to detect misbehaving nodes at forward level instead of the link level, it may fail to detect misbehaving nodes within the presence of: 1) ambiguous collisions, 2) receiver collisions, 3) limited

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 10, October 2018

transmission power, 4) false misbehavior report, 5) collusion (collaborative) of malicious nodes, and 6) partial dropping.

The TWOACK [4] technique is a network layer acknowledgment scheme proposed by Balakrishnan et al. TWACK replace Watchdog scheme by solving two of its weaknesses, named, receiver collision and limited transmission power. In TWOACK, when node forward a packet to its neighbor in a route path, it has to validate whether the packet successfully received by the node that is two hops from it. This achieved by acknowledging every data packet transmitted from source to destination over every three consecutive nodes along the path. As shown in figure 4, node B receives packet 1 from A and forwards it to C, node C (two hops away from A down the route) is required to generate acknowledgement packet (TWOACK). When node C sends the TWOACK packet back to A indicates that B has forwarded packet 1 to C successfully. If A didn't receive TWOACK packet from C within a predefined timeout, then node A marks nodes B and C as misbehaving nodes.

The Delay per Hop Indicator (DelPHI) [5] proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to find every available disjoint route between a sender and a receiver. Then, the delay time and length of each route are calculated and the average delay time per hop along each route is computed. These values are used to identify wormhole. The route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both types of wormhole attack; however, it cannot pinpoint the location of a wormhole. Moreover, because the lengths of the routes are changed by every node, including wormhole nodes, wormhole nodes can change the route length in a certain manner so that they cannot be detected. Sun Choi et al. presented an effective method called Wormhole Attack Prevention (WAP) without using specialized hardware. In WAP All nodes monitor its neighbor's behavior when they send RREQ messages to the destination by using a special list called Neighbor List. When a source node receives some RREP messages, it can detect a route under wormhole attack among the routes. Once wormhole node is detected, source node records them in the Wormhole Node List. Even though malicious nodes have been excluded from routing in the past, the nodes have a chance of attack once more. Therefore, we store the information of wormhole nodes at the source node to prevent them taking part in routing again.

Packet Leash [6] is an approach in which some information in added to restrict the maximum transmission distance of packet. There are two types of packet leashes: geographic leash and temporal leash. In geographic leash, when a node A sends a packet to another node B, the node must include its location information and sending time into the packet. B can estimate the distance between them. The geographic leash computes an upper bound on the distance, whereas the temporal leash ensures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes must have tight time synchronization. The maximum difference between any two nodes' clocks is bounded by Δ, and this value should be known to all the nodes. By using metrics mentioned above, each node checks the expiration time in the packet and determine whether or not wormhole attacks have occurred. If a packet receiving time exceed the expiration time, the packet is discarded.

Unlike Packet Leash, Capkun et al. [7] presented SECTOR, which does not require any clock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD). Node A estimates the distance to another node B in its transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of flight, A detects whether or not B is a neighbor or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash. In order to avoid the problem of using special hardware, a Round Trip Time (RTT) mechanism is proposed by Jane Zhen and Sampalli. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node A to Route Reply (RREP) message receiving Time from a node B. A will calculate the RTT between A and all its neighbors. Because the RTT between two fake neighbors is higher than between two real neighbors, node A can identify both the fake and real neighbors. In this mechanism, each node calculates the RTT between itself and all its neighbors. This mechanism does not require any special hardware and it is easy to implement; however it cannot detect exposed attacks because fake neighbors are created in exposed attacks.

CONCLUSION

Security is one of the most important constraints for the ad hoc network performance. This vulnerability invite attacker to attacking several kinds of attacks on the network resources. These attacks impact on network throughput, performance and lifetime. A lot of research have been done against attacks and required more research to defend the network resources from different attacks by detecting and preventing data from detected attack. Efforts are putting to improve the network security mechanism for smooth network operations against intrusion.

Mobile ad-hoc network needs to take major concern of security due to vulnerable open environment and non-stationary mode. Mostly, offenders focus to attack on victim using these venerable points to affect resources and performance of the networks. Kinds of attack targeted on victim nodes which are influence resources actively and passively. Several works have been done to detect and mitigate such kind of attacks, but still some more work required. In this paper, different activity of intrusion and IDS Schemes are discussed.

REFERENCES

[1]. Mohit Kumar and Rashmi Mishra, "An overview of MANET: History, Challenges and Applications," proceeding of Indian Journal of Computer Science and Engineering, Volumes 3, No. 1, Feb-Mar 2012, ISSN: 0976-5166, pp. 121-125.
[2]. Suresh Singh, Mike 1000, C.S. Raghavendra, " Power-Aware Routing in Mobile Ad-hoc Network.
[3]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA, 2000, pp. 255–265.
[4]. Balakrishnan, K.; Jing Deng; Varshney, V.K., "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp. 2137-2142 Vol. 4, 13-17 March 2005.
Chiu, HS; Wong Lui, "DelPHI: wormhole detection mechanism for ad hoc wireless networks", The 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand, 16-18 January 2013
[5]. Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", Carnegie Mellon University.
[6]. Srdjan Capkun, Levente Buttyan, Jean-Pierre Hubaux, SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks, ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), October 31, 2003, Washington, USA.
[7]. T. Sheltami, A. Al-Roubaiey, E. Shakshuki and A. Mohmoud. Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs. International Journal of Multimedia Systems, Springer, vol. 15, issue 5, 273-282. 2009.
[8]. Abdulsalam Basabaaa, Tarek Sheltamia and Elhadi Shakshukib, "Implementation of A3ACKs intrusion detection system under various mobility speeds", 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)