INTRUSION DETECTION IN MOBILE AD-HOC NETWORK

***ARCHANA SINGH, **DR. RAJESH PATHAK, ***DR.S.P. TRIPATHI**

* HOD Deptt. Of Computer Science GNIT Institute of Technology, Gautam Budh Nagar, U.P.
**A.P. SIET Ghaziabad Research Scholar
***H.O.D. IET Lucknow

ABSTRACT

A mobile Ad-hoc network (Mobile Ad-Hoc Network) is a self-created self-organized and self-administering set of nodes connected via wireless links without the aid of any fixed infrastructure or centralized administrator. Security has become important to mobile ad hoc networks (Mobile Ad-Hoc Network). Due to its unique features such as limited power and limited bandwidth, open nature, lack of infrastructure and central management, node mobility and change of dynamic topology. It is mainly use for many intelligent missions and life-critical applications. However, the broadcast nature of inter-node communications and node mobility in Mobile Ad-Hoc Network make it very challenging to secure. Moreover, their constantly changing topology causes network node density and neighbor relationships to change dynamically. The prevention methods like authentication and cryptography techniques alone are not able to provide the security to these types of networks. Therefore, efficient intrusion detection must be deployed to facilitate the identification and isolation of attacks. The Intrusion Detection Systems utilizes are: (i) both anomaly and misuse detection schemes to identify attacks in Mobile Ad-Hoc Network and

(ii) mobile agents (MAs) to augment each node's intrusion-detection capability. In particular, each node is equipped with local IDS, and MAs will be dispatched periodically or on- demand to augment each node's

IDS. We present the design of these IDS and the overall network structure, as well as the methods for authenticating and dispatching MAs. This paper presents an intrusion detection system (IDS) for Mobile Ad-Hoc Network

Keywords- Intrusion Detection System (IDS), Mobile Agents (MAs), Authentication.

Paper Type- Research Papers

INTRODUCTION

Mobile Ad-hoc network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. Each node moves and operates in a distributed peer-to-peer mode and generating independent data and acting as a router to provide multi-hop communication. Mobile Ad-Hoc Network is ideally suited for potential applications in civil and military environments, such as responses to hurricane, earthquake, tsunami, terrorism and battlefield

conditions. Therefore security is its important aspect in such mission critical applications. The operation of Mobile Ad-Hoc Network does not depend on pre existing infrastructure or base stations. Network nodes in Mobile Ad-Hoc Network are free to move randomly. All network activities such as discovering the topology and delivering data packets have to be executed by the nodes themselves either individually or collectively. The Structure may vary from small, static to a large mobile network. There are two types of Mobile Ad-Hoc Network- closed and open. In a closed Mobile Ad-Hoc Network all mobile nodes cooperate with each other towards a common goal. In an open Mobile Ad-Hoc Network different mobile nodes with different goals share their resources in order to ensure global connectivity. The overall goal of the security solutions for Mobile Ad-Hoc Network is to provide security services including authentication, confidentiality, integrity, anonymity and availability to the mobile users. In order to achieve this goal for the security solution should provide complete protection spanning of the entire protocol stack. We can categories Mobile Ad-Hoc Network security in 5 layers, such as *Application layer, Transport layer, Network layer, Link layer,* and *Physical layer.* However, we only focus on the network layer, which is related to security issues to protect the ad-hoc routing and forwarding protocols. From the security design perspective the Mobile Ad-Hoc Network have no clear line of defense unlikely wired networks that have dedicated routers each mobile node in an ad hoc network may function as a router and forward packets for other peer nodes and wireless channel is accessible to both legitimate network users and malicious attackers. As a result, the boundary that separates the inside network from the outside world becomes blurred. On the other hand, the existing ad hoc routing protocols such as (AODV, DSR) and wireless MAC protocols, such as 802.11, typically assume a trusted and cooperative environment. As a result, a malicious attacker can readily become a router and disrupt network operations by intentionally disobeying the protocol specifications. In this paper we explain various techniques of IDS.

Present Scenario

A. Kathirvel et al. [4] describe the umpiring System for securing the mobile ad- hoc networks from malicious nodes attacks. We consider following systems-

1. Single Umpiring System

In the single umpiring system an additional node is appointed as designated umpires The role of the designated umpires is overhearing both routing message and packet forwarding message in the promiscuous mode. When a designated umpire node is found to be misbehaving – say dropping forwarded packets or changing hop count and sequence number, the corresponding umpire immediately

sends a M-ERROR message to the source and the status bit of guilty node is set to "1" – red flag using M-Flag message.

2. Double Umpiring System

In double umpiring system there are two umpires which monitor the behavior of an intermediate node. The role of the double umpiring system, the designated umpires is overhearing both routing message and packet forwarding message in the promiscuous mode. transmission, the designated umpire immediately sends a M-ERROR message to the source and the status bit of culprit node is set to "1" – red flag using M-Flag message.

3. Triple Umpiring System

In Triple umpiring system, three umpires are used to identify and convict the guilty node. Three umpires in TUS are a node (next/previous immediate node) and two additional nodes is appointed as designated umpires.

It is assumed that the source and destination node are not malicious. Therefore an umpiring system for security for mobile ad hoc network has been proposed- Throughput with single umpire system is greater than DUS and TUS. From throughput and energy point of view SUS has got the benefit. But DUS and TUS we can use the umpire to def the umpire role and take over alternative route if the route fails. We envisage that our system can profitably be used in civilian situations where invariably nodes are lean and energy starved. And acoording to S. Madhavi and T.H. Kim [8] developed an Mobile Intrusion Detection Systems for multi-hop ad-hoc wireless network that is monitor node whose job to detect misbehaving node and packet dropping and packet delaying attack and also According to Marti et al. [11] introduced two extensions to the Dynamic Source Routing Protocol (DSR) to mitigate the effect of routing misbehaviors i.e watchdog and pathrater. The watchdog identifies misbehaving nodes while the pathrater avoids routing packets through these nodes. When a node forwards packets the node's watchdog verifies that the next node in the path and also forwards the packet. The watchdog does this by listening promiscuously to the next hop transmissions. If the next node doesn't forward the packet then it is misbehaving. The watchdog detects the misbehavior and sends a message to the source and notifying it of the misbehaving node. According to S. Sen [12] proposed a "grammatical evolution approach to intrusion detection on mobile ad -hoc networks". They use artificial intelligence based learning technique to explore design space and grammatical evolution technique inspired by natural evolution to detect known attacks on Mobile Ad-Hoc Network such as DOS and route disruption attacks. Intrusion detection programs are evolved for each attack and distributed to each node on the network.

Challenges

A number of constraints and technical difficulties faced by researchers which are described in previous section. These general problem must be consider for further research in this area to propose new technologies for intrusion detection in mobile ad-hoc networks and some of these are-

i. Unlike wired network, the mobile ad-hoc network does not need any infrastructure so it is very difficult to perform any kind of centralized management and control.

ii. Large numbers of sensors are deployed to monitor the network activities in coordinated intrusion detection techniques. And finding optimal position of the sensors requires tactical processing and collecting data from them consumes a lot of network bandwidth.

iii. The resource constraint constitutes another challenge to mobile ad-hoc network. The wireless channel is bandwidth-constrained and shared among multiple networking entities. At the same point computational capabilities of mobile devices are also limited and these devices are powered by batteries with its inherent limitation.

iv. IDS accuracy itself is a critical issue. In Mobile Ad-Hoc Network, the IDS monitor the activities and analyze and compare them against the security rules and accordingly generate the alarm. Because of the dynamic nature of network, most IDS suffer from the false positive and false negative alarm.

v. In the Mobile Ad-Hoc Network, the IDS is so distributed and the node itself is not trusted so IDS does not guarantees to work efficiently and should be should be some trust model a knowledgeable attacker can able to bypass the security rules of IDS so protection of IDS against attacks is required.

Proposed Solutions and Suggestions

To prevent an attacker from spoofing or inserting false data, we sign every MA, the periodic and detection reports, and the anomaly reports from nodes with the MA server's or the nodes' private keys to achieve authenticity and integrity. We also encrypt the MAs with the network-wide symmetric key. The MAs also carry an encrypted function for digital signature to ensure the authenticity of the periodic and detection reports. The node compromised by an attacker can be detected by the local IDS, and the response agent in the IDS will handle the intrusion. If the local IDS is compromised, then the periodically-sent verification MAs will be able to detect the faulty IDS agents, and the MA server will dispatch analysis MAs for diagnosis and response. Malicious nodes can cause service disruption and Denial of- Service (DoS) attacks. There is not an easy way to prevent such nodes from launching attacks, but they can be detected and then removed from the network. We rely on the local IDS at each node to

detect the nodes' malicious behaviors. Since we let a local IDS monitor and detect known intrusions and anomalies on each node, and let MAs aid the detection, once a node identifies a malicious or anomaly behavior, its IDS response agent can evict the compromised node from the network and the neighbor nodes will ignore any messages from the compromised node. Another potential attack is for a node to launch DoS attacks to the MA server, requesting MAs from or sending reports to the MA server. This kind of DoS attacks targeting the MA server can be handled by having the MA server keep path histories of the messages sent to it in order to pinpoint the attacker and restrict the number of times a node can contact it within a certain time duration. Sybil attacks [8] are particularly harmful in Mobile Ad-Hoc Network where a Sybil node illegitimately fakes to have multiple identities in the network. Our MA-based IDS withstands such attacks since each node will need to have a private key and a matching certificate to authenticate its identity. Since each node will have a preloaded private key and certificate, no node can generate the private key and certificate, and pretend to be another node without compromising the node.

References

[1] Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balakrishnan, Member, IEEE, "An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in Mobile Ad-Hoc Network", IEEE Transactions on mobile computing, Vol. 6, NO. 5, May 2007.

[2] Dhanalakshmi, Dr.M.Rajaram ," A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET",IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, Oct,2008.

[3] Zan Kai Chong1, Moh Lim Sim1, Hong Tat Ewe2, and Su Wei Tan ," Separation of Detection Authorities (SDA) Approach for Misbehavior Detection in Wireless Ad Hoc Network",PIERS ONLINE, VOL. 4, NO. 8, 2008.

[4] Ayyaswamy Kathirvel, Rengaramanujam Srinivasan, "A System of Umpires for Security of Wireless Mobile Ad Hoc Network", In *(International Arab Journal of e-Technology, Vol. 1, No. 4, June 2010)* Faculty of Computer Science and Engineering, B.S.Abdur Rahman University, India.

[5] W. Jansen, P. Mell, T. Karygiannis, and D. Marks, "Applying Mobile Agents to Intrusion Detection and Response," in *NIST Interim Report (IR) 6416*, October 1999.

[6] T. Park and K. G. Shin, "Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 4, no. 3, pp. 297–309, May/June 2005.

[7] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT: SoftWarebased ATTestation for Embedded Devices," in *Proceedings of the IEEE Symposium on Security and Privacy*, May 2004.

[8] S.Madhavi and Dr. Tai Hoon Kim "An Intrusion Detection System in Mobile Ad hoc Networks" *International Journal of Security and its Application*, 2, No 3, July 2008.

[9] T. Sander and C. F. Tschudin, "Towards Mobile Cryptography," in *Proceedings of the IEEE Symposium on Security and Privacy*, May 1998.

[10] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad hoc Networks," in *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, January 2002.

[11] S. Marti, T.J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad hoc Networks", *In Proc. ACM/IEEE Int'l Conf. on Mobile Computing and Networking*, Pp. 255-265, 2000.

[12] S.Sen and John Andrew Clark *"A Grammatical Evolution Approach to Intrusion Detection on Mobile Ad hoc Networks"* March 2009, WiSec '09: Proceedings of the Second ACM Conference on Wireless Network Security.