Ontology for MANET Intrusion Detection

[1]Jatinder Singh, [2]Rohit Sharma
[1]Universal Group of Institutions
[2]Sri Guru Teg Bahadur Khalsa College, Anandpur Sahib, Ropar, Punjab, India

Abstract
At present, the security issues on MANET have become one of the primary concerns. The MANET is more vulnerable to attacks as compared to wired networks due to distributed nature and lacks of infrastructure. Those vulnerabilities are nature of the MANET structure that cannot be removed easily. As a result, attacks with malicious intent have been and will be devised to exploit those vulnerabilities and to cripple the MANET Operation. Attacks prevention techniques such as a authentication and encryption, can be used as medium of defense for decreasing the possibilities of attacks. These techniques have a limitation on the effects of prevention techniques in practice and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security measures. For this purpose, there exist a need of mechanism that "detect and response" these type of newer attacks i.e. "Intrusion and Detection". Intrusion detection provide audit and monitoring capabilities that offer the local security to a node and help to perceive the specific trust level of other node. In addition to this ontology is a proven tool for this type of analysis. In this paper, specific ontology has been modeled which aims to explore and to classify current technique of Intrusion Detection System (IDS) aware MANET. To support these ideas, a discussion regarding attacks, IDS architecture and IDS in MANET are presented inclusively and then the comparison among several researches achievement will be evaluated based on these parameters.

I. Introduction

IEEE 802.11 standard specifies "ad hoc" mode as an optional feature, which allows devices to communicate directly with each other in a peer-to-peer manner without any access points. In MANET, no fixed infrastructure, like base station or, mobile switching center is requied. Instead, every possible wireless mobile host within the perimeter of radio link acts as an intermediate switch and participates in setting up the network topology in a self organized way. Ad hoc network supports multi-hop routing, thereby extending the range of mobile nodes well beyond that of their base transceiver. This can extend the range of the wireless LAN form hundreds of feet to miles, depending on the concentration of wireless users. Other advantages include easy installation, less maintenance, flexibility, and it is ideally suited for disaster management (fire, earthquakes etc.), military operations and critical missions. Also, apart from traditional use in office environments, MANET targets domestic networking market as it allows interconnection of various entertainment device at a competitive cost [30].

There are several multi-hop routing protocols have been proposed for MANET, and most popular ones include: Dynamic Source Routing (DSR) , Optimized Link-State Routing (OLSR) , Destination-Sequenced Distance-Vector (DSDV) and Ad Hoc On-Demand Distance Vector (AODV) , Most these protocols rely on the assumption of a trustworthy cooperation among all participating devices; unfortunately, this may not be a realistic assumption in real systems. Malicious nodes could exploit the weakness of MANET to launch various kinds of attacks.

Node mobility on MANET can not be restricted. As results, many IDS solutions have been proposed for wired network, which they are defined on strategic points such as switches, gateways, and routers, can not be implemented on the MANET. The rest of this paper will be structured as follows. Section 2 describes history and background of the IDS in MANET. The Intrusion detection on MANET is presented on section 3. In section 4, we present a discussion regarding the IDS classification. Finally, the ontology for MANET in section 5.

II. History and Background of IDS

Actually, system administrators performed intrusion detection by sitting in front of a console and monitoring user activities. They might detect intrusions by noticing, for example, that a vacationing user is logged in locally or that a seldom-used printer is unusually active. Although effective enough at the time, this early form of intrusion detection was ad hoc and not scalable.

An intrusion-detection system (IDS) can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. Intrusion detection is typically one part of an overall protection system that is installed around a system or device - it is not a stand-alone protection measure.

Depending on the detection techniques used, IDS can be classified into three main categories [6] as follows : 1) signature or misuse based IDS, 2) anomaly based IDS, 3) Specification based IDS, which it is a hybrid both of the signature and the anomaly based IDS.

- The signature-based IDS uses pre-known attack scenarios (or signatures) and compare them with incoming packets traffic. There are several approaches in the signature detection, which they differ in representation and matching algorithm employed to detect the intrusion patterns.
- Meanwhile, the anomaly-based IDS attempts to detect activities that differ from the normal expected system behavior. This detection has several techniques, i.e.: statistics [11], neural networks [12], and other techniques such as immunology, data mining [[14], [15]], and Chi-square test utilization [13].
- The specification-based IDS monitors current behavior of systems according to specifications that describe desired functionality for security-critical entities [24]. A mismatch between current behavior and the specifications will be reported as an attack.

III. Manet Intrusion Detection

There are three focuses in this section: attacks, IDS architectures grouping, and IDS in MANET. The IDS in MANET uses several parameters such as the IDS architectures, the detection techniques (see section 2).

3.1. Attacks

The MANET is susceptible to passive and active attacks . The Passive attacks typically involve only eavesdropping of data, whereas the active attacks involve actions performed by adversaries

such as replication, modification and deletion of exchanged data. In particular, attacks in MANET can cause congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely [[20].

Nodes that perform the active attacks are considered to be malicious, and referred to as compromised, while nodes that just drop the packets they receive with the aim of saving battery life are considered to be selfish [[22],[20]]. In addition, a compromised node may use the routing protocol to the node whose packets it wants to intercept as in the so called black hole attack .

Spoofing is a special case of integrity attacks whereby a compromised node impersonates a legitimate one due to the lack of authentication in the current ad hoc routing protocols . The main result of the spoofing attack is the misrepresentation of the network topology that may cause network loops or partitioning. Lack of integrity and authentication in routing protocols creates fabrication attacks that result in erroneous and bogus routing messages.

Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET .

3.2. IDS Architecture

An IDS is used to detect attempted intrusion into a computer or network. It processes audit data, performs analysis and takes certain set of actions against the intruder, such as blocking them and/or informing the system administrator. Ad hoc networks lacks in centralized audit points, therefore, it is necessary to use the IDS in a distributed manner. This also helps in reducing computation and memory overhead on each node. There are four main architectures on the network [25] , as follows: 1) Standalone IDS, 2) Distributed and Collaborative IDS, 3) Hierarchical IDS, and 4) Mobile Agent for Intrusion Detection Systems.

- In the standalone architecture, the IDS runs on each node to determine intrusions independently. There is no cooperation and no data exchanged among the IDSes on the network. This architecture is also more suitable for flat network infrastructure than for multilayered network infrastructure
- The distributed and collaborative architecture has a rule that every node in the MANET must participate in intrusion detection and response behaving an IDS agent running on them. The IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.
- The hierarchical architecture is an extended version of the distributed and collaborative IDS architecture. This architecture proposes using multi-layered network infrastructures where the network is divided into clusters. The architecture has cluster heads, in some sense, act as control points which are similar to switches, routers, or gate ways in wired networks.
- The mobile agent for IDS architecture uses mobile agents to perform specific task on a nodes behalf the owner of the agents. This architecture allows the distribution of the intrusion detection tasks. There are several advantages using mobile agents , for intrusion detection.

3.3. IDS In Manet

An effective IDS is a key component in securing MANETs. Two different methodologies of intrusion detection are commonly used [[27],29]] anomaly intrusion detection and misuse intrusion detection. Anomaly-detection systems are usually slow and inefficient and are prone to miss insider attacks. Misuse-detection systems cannot detect new types of attack. Hybrid system using both techniques are often deployed in order to minimize these shortcomings [27,28].

VI. Discussion and Summary

The classification among the proposed IDS of MANET can be composed using the parameters discussed in the previous sections , i.e.: architecture, attacks, and IDS detection techniques. Most the MANET IDSes tend to have the distributed architectures and their variants. The IDS architecture may depend on the network infrastructure (see section 3.2). But the most important thing is the reasons the architecture to be configured in distributed manner. As the nature of MANET is so open, attacks source can be generated from any nodes within the MANET itself or nodes of neighboring networks. Unfortunately, this network lacks in central administration. It is difficult for implementing firewall or the IDS on the strategic points.

All attacks type of wired networks is possible in MANET. MANET has also several typical of attacks, which are not available in the traditional wired network, such as selfish attack, black hole attack, sleep deprivation attack and others type of attacks (see section 3.1). These attacks occur because of MANET has vulnerable in the use of wireless link, auto-configuration mechanisms and its routing protocol. The existing MANET IDSes have various methods to detect and to response regarding these attacks. Zhang [23] and Sun [26] proposed the IDSes which were designed for detecting the intrusion activities on the routing protocol of MANET.

V. Ontology for Manet

Research works about ontologies are new and, to some extent inadequate. Simmonds et al. [15] discussed formation of and ontology for network security attacks in general. The concept was discoursed with the focus on wired infrastructure. Quite naturally additional problems faced by a MANET cannot be analyzed with it.

In this paper, an ontology has been demonstrated that is neither target-centric nor, attack specific. As MANET networks are distributive and at the same time collective, a system point of view would be more suitable. So. System that encompasses whole network, processes and other components, is considered as the main class here. Threat is another class that represents a particular state of system. A system is said to be in threat when some properties of the system malfunction. A threat is initiated when some malicious Input affects current state of system. Inputs are generated from Actors, either human or other entities.

Reference

[1] C.E Perkins, E. Belding-Royer. "Ad hoc On-demand Distance Vector (AODV)", Request For Comments (RFC) 3561, 2003

[2] C. Endorf, E. Schultz, J. Mellander, "Intrusion Detection & Prevention", McGraw-Hill, ISBN: 0072229543 (2004)

[3] J. P. Anderson. "Computer Security Threat Monitoring and Surveillance". Technical Report, James P. Anderson Co., Fort Washington, PA, 1980

[4] D.E. Denning, "An Intrusion-Detection Model". IEEE Transactions on Software Engineering, pp. 222- 231, 1987
[5] L. Heberlein, G. Dias, et.al. "A network security monitor". In Proceedings of the IEEE Symposium on Security and Privacy, pp. 296-304, 1990
[6] A. Hijazi, N. Nasser. "Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks". In Wireless and Optical Communications Networks (WOCN), 2005
[7] T. F. Lunt, R. Jagannathan, et al. "IDES: The Enhanced Prototype C a Realtime Intrusion Detection Expert System". Technical Report SRI-CSL-88-12, SRI International, Menlo Park,CA, 1988
[8] M. Esposito, C. Mazzariello, et.al. "Evaluating Pattern Recognition Techniques in Intrusion Detection Systems". The 7th International Workshop on Pattern Recognition in Information Systems, pp. 144-153, 2005
[9] S. Kumar, E. Spafford, "A Pattern Matching Model for Misuse Intrusion Detection". The 17th National Computer Security Conference, pp. 11-21, 1994
[10] P.A. Porras, R. Kemmerer, "Penetration State Transition Analysis C a Rule-Based Intrusion Detection Approach". The 8th Annual Computer Security Application Conference, pp. 220-229, 1992
[11] P. Porras, A. Valdes, "Live Traffic Analysis of TCP/IP Gateways". ISOC Symposium on Network and Distributed System Security, San Diego, CA, 1998
[12] H. Debar, M. Becker, D. Siboni. "A Neural Network Component for an Intrusion Detection System". Proceedings of IEEE Symposium on Research in Security and Privacy, Oakland, CA, pp. 240-250, 1992
[13] N. Ye, X. Li, et.al. "Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data". IEEE Transactions on Systems, Man, and Cybernetics, pp. 266-274, 2001
[14] W. Lee, S.J. Stolfo, K.W. Mok. "A Data Mining Framework for Building Intrusion Detection Models". IEEE Symposium on Security and Privacy (Oakland, California), 1999
[15] G. Florez, S.M. Bridges, R.B. Vaughn, "An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection". The North American Fuzzy Information Processing Society Conference, New Orleans, LA, 2002
[16] Aniruddha Chandra,"Ontology for MANET Security Threats", Electronics and Telecommunication Engineering Departement
[17] Rohit Mangla," Intrusion Detection in MANET", International Journal of Educational Administration, ISSN 0976-5883 vol. 2.
[18] Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah International Journal of Computer Science and Security, Volume (2) : Issue (1) 10
[19] H. Debar, M. Dacier, A.Wespi, "A Revised Taxonomy for Intrusion-Detection Systems". Annales des Telecommunications, pp. 361-378, 2000
[20] L. Blazevic et al. "Self-organization in mobile ad-hoc networks: the approach of terminodes", IEEE Communications Magazine , pp. 166–173, 2001
[21] W. Zhang, R. Rao, et. al. "Secure routing in ad hoc networks and a related intrusion detection problem", IEEE Military Communications Conference (MILCOM), vol. 2, 13–16 pp. 735– 740, 2003
[22] J. Kong et al. "Adaptive security for multi-layer ad-hoc networks". Special Issue of Wireless Communications and Mobile Computing, John Wiley Inter Science Press (2002)
[23] Y. Zhang, W. Lee, "Intrusion detection in wireless ad-hoc networks", The 6th Annual International Conference on Mobile Computing and Networking, pp. 275–283, 2000
[24] C. Ko, J. Rowe, P. Brutch, K. Levitt, "System Health and Intrusion Monitoring Using a hierarchy of Constraints". In Proceedings of 4th International Symposium, RAID, 2001
[25] T. Anantvalee, J. Wu. "A Survey on Intrusion Detection in Mobile Ad Hoc Networks", Book Series Wireless Network Security, Springer, pp. 170 – 196, ISBN: 978-0-387-28040-0 (2007)
[26] B. Sun, K.Wu, U. W. Pooch. "Alert Aggregation in Mobile Ad Hoc Networks". The 2003 ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, 2003
[27] J. S. Balasubramaniyan et al., "An Architecture for Intrusion Detection using Autonomous Agents," Proceedings of the Fourteenth Annual Computer Security Applications Conference, 1998
[28] M. Asaka et al., "A Method of Tracing Intruders by Use of Mobile Agents," in proceedings of the Internet Society, 1999
[29] S. Kumar, E. Spafford, "An Application of Pattern Matchin in Intrusion Detection," Technical Report 94-013, Dept. of Computer Science, Purdue University, 1994
[30] N.Milanovic, M. Malek, A. Davidso, V. Milutinovic,"Routing and Security in mobile Ad hoc Netwoks", IEEE Computer Magazine , vol. 37,no. 2,February 2004.