A SURVEY ON APPLICATION OF IDS IN MANET

Omkar Pattnaik[1] and Binod Kumar Pattanayak[2]
[1]Sinergy Institute of Engineering and Technology, Dhenkanal, Odisha, India
[2]Institute of Technical Education and Research, Siksha 'O'Anusandha University, Bhubaneswar, Odisha, India
E-Mail: bkp_iter@yahoo.co.in

ABSTRACT

Dynamic nature of wireless ad hoc networks imposes a set of challenges to its efficient implementation in a wide range of applications. Quality of Service (QoS) parameters such as bandwidth, delay, power etc. should be optimized in order to provide an improved performance level of ad hoc applications. Security in ad hoc routing is another major concern for efficiency of ad hoc networks. Intrusion detection represents one of such security aspects. Intrusion Detection Systems (IDS) are designed to fulfill the purpose. In this paper, we carry out an extensive survey on IDS exploring the resources available as of today. Our survey includes a study on different types of IDS along with different types of attacks which IDSes target to overcome. We also discuss the underlying architecture of IDS. In addition, we provide an overview of IDS design techniques in the context of Watchdog / Pathrater mechanism. We assume that researchers can benefit from this survey in order for optimal implementation of their research work in the context of IDS in MANETs.

Keywords: MANET, QoS, IDS, attacks.

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a self-configuring dynamic network of mobile devices connected by wireless links set for a specific purpose. In recent years, the use of mobile ad hoc network has increased in comparison with wired network. Quality of service (QoS) is the performance level of a service offered by the network to the user. The goal of QoS provisioning is to achieve a more deterministic network behavior, so that information carried by the network can be better delivered and network resources can be better utilized. The QoS parameters required for communication between the nodes are: delay, throughput, jitter, bandwidth, packet loss etc. Security is another important parameter of QoS in MANET. Security has become one of the major concerns in MANETs. The nature of mobile ad hoc networks poses a range of challenges to the security design. These include an open decentralized peer-to-peer architecture, a shared wireless medium and a highly dynamic topology. The MANET is more vulnerable to attacks as compared to wired network. One of these vulnerabilities is the nature of the MANET structure that cannot be removed. As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious [1]. Therefore, only one compromised node can cause the failure of the entire network. In MANET, both passive and active attacks are possible due to its nature. In case of passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes violate availability, integrity, authentication, and non-repudiation. Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or a network system. The mechanism by which this is achieved is called an Intrusion Detection System (IDS). An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Although there is several intrusion detection techniques developed for wired networks as of today, they are not suitable for wireless networks due to the differences in their characteristics.

Therefore, those techniques must be modified or new techniques must be developed to make intrusion detection effectively in MANETs.

2. BACKGROUND OF INTRUSION DETECTION SYSTEM (IDS)

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 a part of an overall protection system that is installed around a system or device and it is not a stand-alone protection measure [1]. The purpose of intrusion detection is to serve as an alarm mechanism for a computer system or a network. It provides information of unwanted or misbehaving elements and isolates those elements to deny them from the computer or network resources. It is possible to identify three main modules in an IDS: a Monitoring Module, controlling the collection of data, an Analysis Module deciding if the data collected indicate an intrusion or not, and a Response Module managing the response actions to the intrusion [Figure-1]. Some assumptions are made in order for intrusion detection systems to work [2]. The First assumption is that user and program activities are observable. The second assumption, which is more important, is that normal and intrusive activities must have distinct behaviors, as intrusion detection must capture and analyze system activity to determine if the system is under attack. Depending on the detection techniques used, IDS can be classified into three main categories [3]: **1)** signature or misuse based IDS, **2)** anomaly based IDS, **3)** specification based IDS, which is a hybrid of both 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. The detection approaches, such as expert system [4], pattern recognition [5], colored petrinets [6], and state transition analysis [7] are grouped on the misuse.

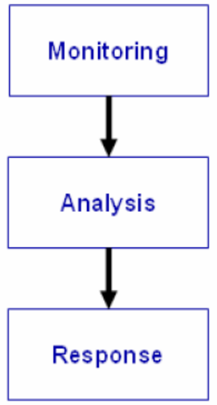

Figure-1. IDS basic modules.

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 [8], neural networks [9], and other techniques such as immunology [10], data mining ([11], [12]), and Chi-square test utilization [13]. Moreover, a good taxonomy of wired IDSes was presented by Debar [14].

The specification-based IDS monitors' current behavior of systems according to specifications that describe desired functionality for security-critical entities [15]. A mismatch between current behavior and the specifications will be reported as an attack. Anomaly detection [Figure-2] bases its idea on statistical behavior modeling and anomaly detectors look for behavior that deviates from normal system use. A typical anomaly detection system takes in audit data for analysis. The audit data is transformed to a format statistically comparable to the profile of a user. The user's profile is generated dynamically by the system (usually using a baseline rule laid by the system administrator) initially and subsequently updated based on the user's usage. Thresholds are normally always associated to all the profiles [16]. If any comparison between the audit data and the user's profile resulted in deviation crossing a threshold set, an alarm of intrusion is declared. This type of detection systems is well suited to detect unknown or previously not encountered attacks.

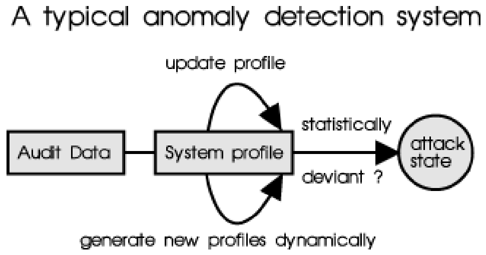

Figure-2. Example of anomaly detection system.

The second type of model bases its detection upon a comparison of parameters of the user's session and the user's commands to a rule base of techniques used by attackers to penetrate a system. Known attack methods are what this model looks for in a user's behavior. Since this model looks for patterns known to cause security problems, it is called a "misuse" detection model [Figure-3].

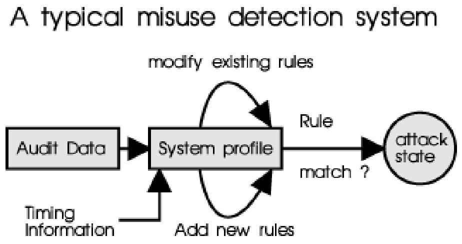

Figure-3. Example of a misuse detection system.

It is obvious that the enemies, knowing that intrusion prevention and detection systems are in our networks, will attempt to develop and launch new types of attacks. In anticipation of these trends, IDS researchers are designing techniques for combining anomaly and misuse detection, and system architecture for distributed and coordinated intrusions.

3. INTRUSION DETECTION IN MANETs

In this section, we present an overview of the types of attack possible in MANETs. Also we focus on the architecture of the IDS in MANETs in next section. In MANETs, basically two types of attack is commonly observed like: Passive attack and Active attack. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Active attacks, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes, violate availability, integrity, authentication, and non-repudiation. [18].

3.1. Intrusion detection in a MANET- attack models

The analysis of existing attack models can facilitate the extraction of effective features, which turns out to be one of the most important steps in building IDS. The following are representative types of attacks in the context of a MANET IDS:

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 ([19], [20]). 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 ([21], [22], [23]) that result in erroneous and bogus routing messages. 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* ([24], [25]). A selfish node affects the normal operation of the network by not participating in the routing or by not forwarding packets. In addition, a compromised node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept as in the so called *black hole attack* ([26], [27]). *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 ([28], [29]). A *routing table overflow attack* and *sleep deprivation attack* are two other types of the DoS attacks [30]. In the routing table overflow attack, an attacker attempts to create routes to passive nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node. *Routing Logic Compromise*: In routing protocols, typical attack scenarios include black hole, routing update storm, fabrication, and modification of various fields in routing control packets (for example, route request message, route reply message, route error message, etc.) during different phases of routing procedures. All these attacks can lead to serious malfunctioned in a MANET [31]. *Traffic Distortion*: This includes attacks such as packet dropping, packet corruption, and data flooding, and so on. Motivated by their different objectives, attackers may take different actions to manipulate packets. For example, attackers may randomly, periodically, or selectively drop received packets to selfishly save power or intentionally prevent other nodes from receiving data [31]. There are also more sophisticated routing attacks. Compared to the simple attacks described above, these sophisticated attacks are much harder to detect and to prevent, i.e., *wormhole attacks* (two compromised nodes create a tunnel that is linked through a private connection and thus they by-pass the network [[32], [33]]), *rushing attacks* [34] and *Sybil attacks* [35].

4. ARCHITECTURE FOR IDS IN MANETs

The IDS can be configured based on the network infrastructure: *flat* or *multi-layer*. The optimal IDS architecture for the MANET may depend on the network infrastructure itself. There are some classification of architectures on the network [36], 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 run 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 respond by having 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, acting 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 node on behalf the agents. This architecture allows the distribution of the intrusion detection tasks. There are several advantages using mobile agents [[37], [38]], for intrusion detection.

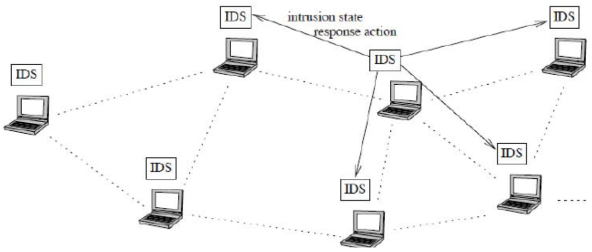

Figure-4. Architecture of IDS in MANET.

5. IDS TECHNIQUES FOR MANET

The solutions to the extensions of the DSR routing protocol to IDS have been already proposed in earlier days. Here we describe another technique for detection and prevention of IDS in MANET. We address a modified version of the *Watchdog / Pathrater* mechanism, which was first proposed in 6th International Conference on Mobile Computing and Networking [39]. The Watchdog/Pathrater is a solution to the problem of selfish (or “misbehaving”) nodes in MANET. The system introduces two extensions to the DSR algorithm to mitigate the effects of routing misbehavior: the Watchdog, to detect the misbehaving nodes and the Pathrater, to respond to the intrusion by isolating the selfish node from the network operation. Watchdog runs on each node. When a node forwards a packet, the node’s watchdog module verifies that the next node in the path also forwards the packet. The Watchdog does this by listening in promiscuous mode to the next node’s transmissions. If the next node does not forward the packet, then it is considered to be misbehaving and is reported. This is done by sending an alarm message to the other nodes on its friends list. When those nodes receive the alarm message, they evaluate it and change the reputation of the accused node only if the alarm source is fully trusted or the same node was accused by several partially trusted nodes. If the Watchdog module that detected the misbehaving node is not in the same node that is acting as source node for the packets, then it sends a message to the source identifying the misbehaving node. The Pathrater module uses the information generated by Watchdog to select a better route to deliver the packets, avoiding the selfish nodes.

6. CONCLUSIONS

Intrusion detection systems, if well designed effectively can identify malicious activities and help to offer adequate protection. Therefore, an IDS has become an indispensable component to provide defense-in-depth security mechanisms for MANETs. In this paper, we perform a survey on existing intrusion detection techniques in the context of MANETs. Since Intrusion prevention alone is not sufficient to achieve security in a network, we have hereby presented a way to manage MANET security, by enhancing the existing secure protocols adding the component of Malicious nodes, not only in determining the route for sending packets, but also avoiding attempts of Denial-of-Service from Malicious Nodes. An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. However, attackers may try to attack the IDS system itself, which may be addressed in future.

REFERENCES

[1] A Survey on MANET Intrusion Detection: Satria Mandala satriamandala@hotmail.com Faculty of Science and Technology, Department of Informatics Engineering, State Islamic University of Malang Jl. Gajayana 50 Malang, Indonesia, Md. Asri Ngadi dr.asri@utm.my Faculty of Computer Science and Information System, Department of Computer System and Communication, Universiti Teknologi Malaysia (UTM) Skudai - Johor, 81310, Malaysia.

[2] Y. Zhang, W. Lee and Y. Huang. 2003. Intrusion Detection Techniques for Mobile Wireless Networks. ACM/Kluwer Wireless Networks Journal (ACM WINET). 9(5).

[3] A. Hijazi and N. Nasser. 2005. Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks. In Wireless and Optical Communications Networks (WOCN).

[4] T. F. Lunt and R. Jagannathan, *et al*. 1988. IDES: The Enhanced Prototype C a Realtime Intrusion- Detection Expert System. Technical Report SRI-CSL-88-12, SRI International, Menlo Park, CA.

[5] M. Esposito and C. Mazzariello, *et al*. 2005. Evaluating Pattern Recognition Techniques in Intrusion Detection Systems. The 7th International Workshop on Pattern Recognition in Information Systems. pp. 144-153.

[6] S. Kumar and E. Spafford. 1994. A Pattern Matching Model for Misuse Intrusion Detection. The 17th National Computer Security Conference. pp. 11-21.

[7] P.A. Porras and R. Kemmerer. 1992. Penetration State Transition Analysis C a Rule-Based Intrusion Detection Approach. The 8th Annual Computer Security Application Conference. pp. 220-229.

[8] P. Porras and A. Valdes. 1992. Live Traffic Analysis of TCP/IP Gateways. ISOC Symposium on Network and Distributed System Security. San Diego, CA, 1998-9. H. Debar, M. Becker and 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.

[9] S. Forrest, S.A. Hofmeyr and A. Somayaji. 1997. Computer Immunology. Communications of the ACM. pp. 88-96.

[10] W. Lee, S.J. Stolfo and K.W. Mok. 1999. A Data Mining Framework for Building Intrusion Detection Models. IEEE Symposium on Security and Privacy. Oakland, California.

[11] G. Florez, S.M. Bridges and R.B. Vaughn. 2002. An Improved Algorithm for Fuzzy Data Mining for Intrusion Detection. The North American Fuzzy Information Processing Society Conference, New Orleans, LA.

[12] N. Ye and X. Li, *et al*. 2001. Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data. IEEE Transactions on Systems, Man, and Cybernetics. pp. 266-274.

[13] H. Debar, M. Dacier and A. Wespi. 2000. A Revised Taxonomy for Intrusion-Detection Systems. Annales des Telecommunications. pp. 361-378.

[14] C. Ko, J. Rowe, P. Brutch and K. Levitt. 2001. System Health and Intrusion Monitoring Using a hierarchy of Constraints. In: Proceedings of 4th International Symposium, RAID.

[15] Intrusion Detection in Wireless Ad-Hoc Networks: Foong Heng Wai hengwai.foong@nus.edu.sg> Yin Nwe Aye <yinnweay@comp.nus.edu.sg> Ng Hian James nghianja@comp.nus.edu.sg: CS4274 INTRODUCTION TO MOBILE COMPUTING.

[16] Sundaram A. An introduction to Intrusion detection, http://www.acm.org/crossroads/xrds2-4/intrus.html.

[17] A.J. Menezes, S.A. Vanstone and P.C. Van Oorschot. 2001. Handbook of Applied Cryptography. CRC Press, Inc., USA.

[18] J. Hubaux, L. Buttya´n and S. Capkun. 2001. The quest for security in mobile ad hoc networks. The 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing.

[19] P. Papadimitratos, Z.J. Haas and E.G. Sirer. 2002. Path set selection in mobile ad hoc networks. The Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing. pp. 1-11.

[20] B. DeCleene, *et al*. 2001. Secure group communications for wireless networks. IEEE Military Communications Conference.

[21] C.E Perkins and E. Belding-Royer. 2003. Ad hoc On-demand Distance Vector (AODV). Request for Comments (RFC) 3561.

[22] S. Bo, W. Kui and U.W. Pooch. 2004. Towards adaptive intrusion detection in mobile ad hoc networks. IEEE Global Telecommunications Conference. pp. 3551-3555.

[23] L. Blazevic, *et al*. 2001. Self-organization in mobile ad-hoc networks: the approach of terminodes. IEEE Communications Magazine. pp. 166-173.

[24] J. Kong, *et al*. 2002. Adaptive security for multi-layer ad-hoc networks. Special Issue of Wireless Communications and Mobile Computing, John Wiley Inter Science Press.

[25] P. Kyasanur and N. Vaidya. 2003. Detection and handling of MAC layer misbehavior in wireless networks. International Conference on Dependable Systems and Networks. pp. 173-182.

[26] Y. Zhang W. Lee. 2000. Intrusion detection in wireless ad-hoc networks. The 6th Annual International Conference on Mobile Computing and Networking. pp. 275-283.

[27] C. Douligeris and A. Mitrokosta. 2004. DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer Networks. The International Journal of Computer and Telecommunications Networking. 44(5): 643-666.

[28] C.M. Chlamtac and J.J.-N. Liu. 2003. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks 1.

[29] H. Yang and H.Y. Luo, *et al*. 2004. Security in Mobile Ad Hoc networks: challenges and solutions. IEEE Wireless Communications. pp. 38-47.

[30] Intrusion detection techniques in mobile ad hoc and wireless sensor networks: bo sun and lawrence osborne, lamar university yang xiao, the university of alabama sghaier guizani, university of quebec at trois-rivieres.

[31] Y. Hu, A. Perrig and D. Johnson. 2003. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In: Proceedings of IEEE INFOCOM'03.

[32] Y. Hu, A. Perrig and D. Johnson. 2002. Ariadne: a secure on-demand routing protocol for ad hoc networks. ACM MOBICOM.

[33] Y. Hu, A. Perrig and D. Johnson. 2003. Rushing attacks and defense in wireless ad hoc network routing protocols. In: Proceedings of ACM Mobi Com Workshop - WiSe'03.

[34] J. R. Douceur. 2002. The sybil attack. The 1st International Workshop on Peer-to-Peer Systems. pp. 251-260.

[35] T. Anantvalee and J. Wu. 2007. 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).

[36] A.J. Menezes, S.A. Vanstone and P.C. Van Oorschot. 2001. Handbook of Applied Cryptography. CRC Press, Inc., USA.

[37] C. Krugel and T. Toth. 2001. Applying mobile agent technology to intrusion detection. In: ICSE Workshop on Software Engineering and Mobility.

[38] S. Marti, T.J. Giuli, K. Lai and M. Baker. 2000. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: 6th International Conference on Mobile computing and Networking, OBICOM'00. pp. 255-265, Aug.