Detection Techniques in MANET

Asma Ahmed[1], **S. Razak**[2], **A. Hanan**[2], **Izzeldin Osman**[3]
[1]Faculty of Computer Science and Information System, Universiti Technologi Malaysia, Johor, Malaysia
[2]Department of Computer Science Universiti Technologi Malaysia, Johor, Malaysia
[3]Faculty of Computer Science, Sudan University Science and Technology, Khartoum, Sudan

Abstract - *In the recent years, the security issues on Mobile ad hoc network (MANET) have become one of the primary concerns. Because of the mobility nature, MANET is more vulnerable to be attacked than wired network. Attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks. However, encryption and authentication cannot defend against compromised mobile nodes which carry the private keys. Intrusion detection techniques (IDS) the second mechanism to detect and response the attack which successfully penetrated the prevention mechanisms. The main categories of these techniques are anomaly-based detection, signature-based detection and specification-based detection. In this paper the different detection techniques- anomaly detection, signature detection and specification-based detection- are classified, as well as comparative discussion of these different techniques.*

Keywords: MANET, Anomaly Detection, Signature Detection, Specification-based Detection.

1 Introduction

The Internet and computer networks are exposed to an increasing number of security threats. Mobile ad hoc network (MANET) is vulnerable to security attacks due to its features of open medium, dynamic changing topology, cooperative algorithms and lack of cartelized monitoring. The flexibility provided by the open broadcast medium and cooperativeness of the mobile devices introduces new security risks. Security services, such as authentication services and access controls, can enhance the security of ad hoc networks. Nevertheless, these preventive mechanisms alone cannot deter all possible attacks (e.g., insider attackers possessing the key). Therefore, it is necessary to have other security mechanisms to deal with misbehaving insider nodes that possess the valid key and access rights. As result, intrusion detection is an indispensable part of security for MANET.

There are several techniques can be applied for the detection of attacks against routing protocols in MANET. The main categories of these techniques are: anomaly-based detection, misuse-based detection and specification-based detection [1]. These techniques apply to each of the routing protocols such as Ad hoc on-demand distance vector (AODV)[27], Dynamic source routing (DSR)[26], Optimized link state routing (OLSR)[10], and potentially other infrastructure protocols used in MANET.

The aim of this paper is to classify current techniques of Intrusion Detection System (IDS) and comparison between these detection techniques.

The paper is organized as follows Section 2 present the concept of prevention mechanisms extends with the limitation of these mechanisms. Section 3 provides an overview of IDS MANET as well as discusses the different detection techniques; these are anomaly-based, signature-based and specification-based. Comparison discussion between these detection techniques is presented in Section 4. Section 5 concludes the paper.

2 Prevention mechanisms

Prevention mechanism is used to secure network against external attacks, where it can be achieved by authenticating users and nodes [2][3][4], and by securing routing protocols used to create routes between nodes[5][6][7]. By signed the routing messages by each node, a large number of attacks can be prevented or eliminated, example of such attacks are:

-Spoofing attacks: Attacks in which nodes send routing messages pretending to be a different node.

-Modifying attacks: Attacks in which nodes modify routing messages in transit with the intention of misleading other nodes.

Modifying the routing protocols to require node authentication is a viable approach but has some limitations: firstly, it increases the overhead since it increases the size of routing messages and the amount of processing needed to process each routing message. Further, every node needs to verify the authenticity of the incoming routing messages.
However, these techniques in general they are designed for a set of known attacks. However, encryption and authentication cannot defend against compromised mobile nodes which carry the private keys. For this reason, there is a need of second mechanism to detect and response the attack that successfully penetrated the prevention mechanisms.

3 Intrusion Detection in MANET

Intrusion detection techniques (IDS) are a valuable technology to protect target systems and networks against malicious activities. Detection and response mechanisms are used to secure network against internal attacks. This can be achieved using intrusion detection systems [8][9]. IDS should be able to detect the malicious activities of attackers who successfully penetrated the prevention mechanisms.
Many intrusion detection systems have been proposed in traditional wired networks, where all traffic must go through switches, routers, or gateways. Hence, IDS can be added to and implemented in these devices easily [12][13]. On the other hand, MANET does not have such devices. Moreover, the medium is wide open, so both legitimate and malicious users can access it. Furthermore, there is no clear separation between normal and abnormal activities in a mobile environment. Since nodes can move arbitrarily, false routing information could be from a compromised node or a node that has outdated information. Thus, the current IDS techniques on wired networks cannot be applied directly to MANET.
Some assumptions are made in order for the intrusion detection systems to work in MANET [14]. 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.
Several techniques can be applied for the detection of attacks against routing protocols. These techniques can be divided into the main categories of: anomaly-based detection, signature-based detection and specification-based detection [1]. These techniques apply to each of the routing protocols such as AODV, DSR, OLSR, and potentially other infrastructure protocols used in MANET (e.g. multicast, session management).

3.1 Anomaly-Based Detection

An Anomaly-based intrusion detection System, is a system for detecting computer intrusions by monitoring system activity and classifying it as either normal or anomalous. This technique tries to detect attacks by looking at activities that vary from the normal expected behavior. Detection techniques can be classified into three main categories [25]:

- Statistical-based.
- Knowledge-based.
- Machine learning-based.

Defining normal behavior major challenge in anomaly detection. Normal behavior can change over time and intrusion detection systems must be kept up to date. False positive – the normal activities that are detect as anomalies by IDS – can be high in anomaly-based detection. On the other hand, anomaly-based detection is capable for detecting previously unknown attacks. This is very important in an environment where new attacks and new vulnerabilities of system are announced constantly.

3.2 Misuse-Based Detection

Misuse-based or signature-based intrusion detection compares known attack signatures with current system activities. Generally misuse-based intrusion detection preferred by commercial IDSs since it is efficient and has a low positive rate.
Misuse detection provides very good detection results for specified, well-known attacks. However, they are not capable of detecting new, unfamiliar intrusions, even if they are built as minimum variants of already known attacks. The system is only as strong as its signature database, and this needs frequent updating for new attacks.

3.3 Specification-Based Detection

The specification-based intrusion detection technique [15] is usually based on building finite state

machines that reflect the expected behavior of the node. The implementation of this idea can be done by monitoring execution such program or protocol respect to the expected behavior. Specification-based intrusion detection technique is introduced as promising alternative that combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with lower false positive rate. It can detect new attacks that do not follow the system specifications. Moreover, it does not trigger false alarm when the program or protocol has unusual but legitimate behavior, since it uses the legitimate specifications of the program or protocol [28]. In specification-based a detector needs to monitor a node very closely and maintain information about the messages sent and received by the node. The detector then also needs to perform similar calculations as performed by a node executing the routing protocol. Therefore the complexity of the detector is typically similar to the complexity of executing the routing protocol itself. This increases the detector complexity, and the data that needs to be stored on the detector to a level that may not be acceptable. Another problem with specification-based detection is danger from misinterpretation of the protocol when the protocol is modeled in detail. This will lead to false alarms because the alarm may be due to a misinterpretation of the protocol in the detector finite state machine. To avoid this problem it has been proposed to simplify detectors by only modeling key characteristics of the protocol and not necessarily every detail. This decreases complexity and simplifies the detector but leaves open the possibility that an attack exploiting the portions of the protocol behavior that are not modeled by the detector will go undetected.

4 Analysis

IDSs on MANET use a variety of intrusion detection methods. The previous discussion illustrates the challenges associated with each of intrusion detection techniques. Anomaly-based detection systems implemented in MANET. Unfortunately, mobility of MANET increases the rate of false positives in these systems. The main benefit of anomaly-based detection techniques is their potential to detect previously unseen intrusion events. Misuse-based detection provides very good detection results for specified, well-known attacks. However, they are not capable of detecting new, unfamiliar intrusions, even if they are built as minimum variants of already known attacks. Updating of attack signatures is an important problem for this approach. Specification-based detection can detect routing attacks against routing protocols with low rate of false positives. However, it cannot detect some kind of attacks, such as DoS attacks. Table1 illustrate the characteristics of each technique.

Table1: Anomaly, Misuse and specification detection

Method	Characteristics
Anomaly-based	- capable for detecting previously unknown attacks - High false positive
Misuse-based	- very good detection results for specified, well-known attacks. - not capable of detecting new attacks.
Specification-based	- detection of known and unknown attacks. - low false positive. - needs to monitor a node very closely. - complsexity of the detector. - Cannot detect DoS attacks

Two key aspects concern the evaluation, and thus the comparison, of the performance of alternative intrusion detection approaches: these are the efficiency of the detection process, and the cost involved in the operation.

5 Discussion and Summary

Mobile ad hoc networks are attractive technology for many applications. However, this flexibility introduced new security risks. Since prevention techniques are never enough, intrusion detection systems (IDSs) are generally used to complement other security mechanisms. Intrusion detection for MANET is complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and lack of central monitoring points. These different characteristics of MANET make conventional IDSs ineffective and inefficient for this new environment.

Recently, many researchers have been working on developing new IDSs for MANET. New approaches need to be developed or else existing approaches need to be adapted for MANETs. This paper, briefly explored the various intrusion detection methods suggested by the authors and also analyzed some challenges and problems of each method in MANET. There is an utmost need of a general foundation for all intrusion detection and supporting activities that can able to adapt dynamic network conditions. The requirement of the system like high security and low bandwidth should be satisfied by the IDS. Also the IDS that are able to detect known and unknown attacks should be considered.

References

[1] A. Mishra, K. Nadkarni, and A. Patcha. "Intrusion Detection in Wireless Ad Hoc Networks". IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.

[2] Douceur, J. R. (2002). The Sybil Attack. In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems. London, UK: Springer-Verlag. ISBN 3540441794.

[3] Capkun, S., Buttyan, L. and Hubaux, J.-P. (2003). Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing. ISSN 1536-1233.

[4] Yi, S. and Kravets, R. (2003). MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks. In 2nd Annual PKI Research Workshop Program (PKI 03.

[5] Xu, Y. and Xie, X. (2008). Security analysis of routing protocol for MANET based on extended Rubin logic. Sanya, China.

[6] Kim, J. and Tsudik, G. (2009). SRDP: Secure route discovery for dynamic source routing in MANETs. Ad Hoc Networks. ISSN 15708705.

[7] Yu, M., Zhou, M. and Su, W. (2009). A secure routing protocol against byzantine attacks for MANETs in adversarial environments. IEEE Transactions on Vehicular Technology. ISSN 00189545.

[8] Rao, R. and Kesidis, G. (2003). Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited. Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE. 5,2957-2961.

[9] Subhadrabandhu, D., Sarkar, S. and Anjum, F. (2004). E_cacy of misuse detection in ad hoc networks. Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on, 97-107. doi: 10.1109/SAHCN.2004.1381907.

[10] T. Clausen, P. Jaquet, et.al. "Optimized link state routing protocol". Internet Draft, draft-ietfmanet-olsr 06.txt, work in progress, 2001.

[11] G. Vigna, S. Gwalani, et al., "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks," in Proceedings of the Annual Computer Security Applications Conference (ACSAC), Tucson, AZ, December, , pp. 16–27 2004.

[12] Y. F. Jou, F. Gong, et al.. "Design and Implementation of a Scalable Intrusion Detection System for the Protection of Networks Infrastructure". Proceedings of DARPA Information Survivability Conference and Exposition, Vol. 2, pp. 69-83, January 2000.

[13] E. Y. K. Chan et al., "IDR: An Intrusion Detection Router for Defending against Distributed Denial-of-Service (DDoS) Attacks". Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks (ISPAN'04), pp. 581-586, May 2004.

[14] Y. Zhang, W. Lee, and Y. Huang. "Intrusion Detection Techniques for Mobile Wireless Networks". ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[15] C.Y. Tseng, P. Balasubramanyam, et al., "A Specification-Based Intrusion Detection System For AODV," in Workshop on Security in Ad Hoc and Sensor Networks (SASN)'03, 2003.

[16] C.K.Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems," Prentice Hall Publications, 2002.

[17] S. Lee, B. Han, and M. Shin, "Robust routing in wireless ad hoc networks," in ICPP Workshops, pp.73, 2002.

[18] Y. A. Huang and W. Lee, "Attack analysis and detection for ad hoc routing protocols," in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.

[19] X. Wang, T. Lin and J. Wong, "Feature selection in intrusion detection system over mobile ad-hoc network," Technical Report, Computer Science, Iowa State University, 2005.

[20] J. Binkley and W. Trost. “Authenticated ad hoc routing at the link layer for mobile systems”. Wireless Networks, 7(2): 139–145, 2001.
[21] Y. C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” in Eighth Annual International Confer-ence on Mobile Computing and Networking (Mobi- Com 2002), pp. 12-23, Sept. 2002.
[22] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. B. Royer, “Authenticated routing for ad hoc networks,” IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610,Mar. 2005.
[23] Y. C. Hu and A. Perrig, “A survey of secure wireless ad hoc routing,” IEEE Security & Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.
[24] H. Deng, W. Li, and D. P. Agrawal, “Routing security in ad hoc networks,” IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
[25] Lazarevic A, Kumar V, Srivastava J. Intrusion detection: a survey, Managing cyber threats: issues, approaches, and challenges. Springer Verlag; 2005. p. 330.
[26] D.B. Johnson, D.A. Maltz, et.al. “The dynamic Source Routing Protocol for Mobile Ad hoc Networks (DSR)”. Internet Draft, draft-ietf-manet-dsr-07.txt, work in progress, 2002.
[27] C.E Perkins, E. Belding-Royer. “Ad hoc On-demand Distance Vector (AODV)”, Request For Comments (RFC) 3561, 2003.
[28] uppuluri P, Sekar R. “Experience with Specification-Based Intrusion Detection. In Proc of the 4th Int Symp on Recent Adv in Intrusion Detect LNCS 2212: 172-189. 2001.