International Research Journal of Emerging Trends in Multidisciplinary
ISSN 2395-4434
Volume 1, Issue 5 July 2015
www.irjetm.com

Intrusion Detection on Manets

K.Sreenivasa Ravi

P.Varshitha (pulimivarshitha@gmail.com)

G.Subramanyam (subramanyamg98@gmail.com)

ABSTRACT

In recent years mobile ad hoc networks (MANETs) have become a very popular research topic. By providing communications in the absence of a fixed infra-structure MANETs are an attractive technology for many applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. However, this flexibility introduces new security risks. Since prevention techniques are never enough, intrusion detection systems (IDSs), which monitor system activities and detect intrusions, are generally used to complement other security mechanisms. Intrusion detection for MANETs is a complex and difficult task mainly due to the dynamic nature of MANETs, their highly constrained nodes, and the lack of central monitoring points. Conventional IDSs are not easily applied to them. New approaches need to be developed or else existing approaches need to be adapted for MANETs. This chapter outlines issues of intrusion detection for MANETs and reviews the main solutions proposed in the literature.

1. INTRODUCTION

Manets is a collection of wireless mobile nodes forming a temporary network without use of any existing network. Routing is one of the core problems of networking for delivering data from one node to another. It allows all the wireless networks within range to communicate with each other; it is possible for small group of devices. But performance degrades as the number of devices grows. A large adhoc networks becomes difficult to manage. Wireless network is seen as one of the fastest growing trends in technology. The flexibility that this network offers has attracted many people.

It is a responsibility of the network developer to ensure and enforce a secured network. Intrusion detection system (IDS) plays a very important role in detecting different types of attacks. The main function of intrusion detection is to protect the network, analyze and find out intrusions among normal audit data. Although there is a number of intrusion detection techniques designed for traditional wired networks, they may not be suitable if applied to mobile ad hoc network due to the differences in their characteristics. Therefore, those techniques must be modified or new techniques must be developed to make intrusion detection work effectively in MANETs

2. ATTACKS AGAINST AD HOC NETWORKS

While a wireless network is more versatile than a wired one, it is also more vulnerable

`

to attacks. This is due to the very nature of radio transmissions, which are made on the air.

On a wired network, an intruder would need to break into a machine of the network or to physically wiretap a cable. On a wireless network, an adversary is able to eavesdrop on all messages within the emission area, by operating in promiscuous mode and using a packet sniffer (and possibly a directional antenna). There is a wide range of tools available to detect, monitor and penetrate an IEEE 802.11 network, such as NetStumbler, AiroPeek, Kismet, Airsnot and Etheral [1]. Hence, by simply being within radio range, the intruder has access to the network and can easily intercept transmitted data without the sender even knowing (for instance, imagine a laptop computer in a vehicle parked on the street eavesdropping on the communications inside a nearby building). As the intruder is potentially invisible, it can also record, alter, and then retransmit packets as they are emitted by the sender, even pretending that packets come from a legitimate party.

Furthermore, due to the limitations of the medium, communications can easily be perturbed; the intruder can perform this attack by keeping the medium busy sending its own messages, or just by jamming communications with noise.

2.1 Incorrect traffic generation

This category includes attacks which consist in sending false control messages: i.e. control messages sent on behalf of another node (identity spoofing), or control messages which contain incorrect or outdated routing information. The network may exhibit Byzantine behaviour, i.e. conflicting information in different parts of the network. The consequences of this attack are degradation in network communications, unreachable nodes, and possible routing loops.

2.1.1 Cache poisoning

As an instance of incorrect traffic generation in a distance vector routing protocol, an attacker node can advertise a zero metric for all destinations, which will cause all the nodes around it to route packets toward the attacker node. Then, by dropping these packets (black hole attack) the attacker causes a large part of the communications exchanged in the network to be lost. In a link state protocol, the attacker can falsely declare that it has links with distant nodes. This causes incorrect routes to be stored in the routing table of legitimate nodes, also known as cache poisoning.

2.2 Incorrect traffic relaying

Network communications coming from legitimate, protocol-compliant nodes may be polluted by misbehaving nodes.

2.2.1 Black hole attack

An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order reducing the quantity of routing information available to the other nodes. This is called black hole attack by Hu et al. and is a “passive” and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets for a specified destination, a

`

packet every n packets, a packet every t seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

2.2.2 Message tampering

An attacker can also modify the messages originating from other nodes before relaying them, if a mechanism for message integrity (i.e. a digest of the payload) is not utilized.

2.2.3 Replay attack

As topology changes, old control messages, though valid in the past, describe a topology configuration that no longer exists. An attacker can perform a replay attack by recording old valid control messages and re-sending them, to make other nodes update their routing tables with stale routes. This attack is successful even if control messages bear a digest or a digital signature that does not include a timestamp [1].

3. Intrusion Detection System (IDS)

Many historical events have shown that intrusion prevention techniques alone, such as encryption and authentication, which are usually a first line of defence, are not sufficient. As the system become more complex, there are also more weaknesses, which lead to more security problems. Intrusion detection can be used as a second wall of defence to protect the network from such problems. If the intrusion is detected, a response can be initiated to prevent or minimize damage to the system. 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 behaviours, as intrusion detection must capture and analyze system activity to determine if the system is under attack. Intrusion detection can be classified based on audit data as either host-based or network-based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis. Based on detection techniques, IDS can also be classified into three categories as follows [3]

- **Anomaly detection systems**: The normal profiles (or normal behaviours) of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.
- **Misuse detection systems:** The system keeps patterns (or signatures) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.
- **Specification-based detection:** The system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints.

`

International Research Journal of Emerging Trends in Multidisciplinary
ISSN 2395-4434
Volume 1, Issue 5 July 2015
www.irjetm.com

4. Sample Intrusion Detection Systems for MANETs

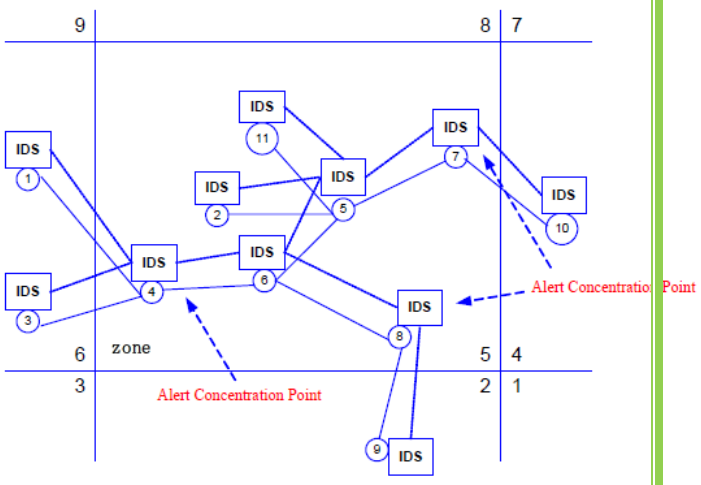
Since the IDS for traditional wired systems are not well-suited to MANETs, many researchers have proposed several IDS especially for MANETs, which some of them will be reviewed in this section.

PROPOSED IDSs

IDSs on MANETs use a variety of intrusion detection methods. The most commonly proposed intrusion detection method to date is specification-based detection. This can detect attacks against routing protocols with a low rate of false positives. However, it cannot detect some kind of attacks, such as DoS attacks. There are also some anomaly-based detection systems implemented in MANETs. Unfortunately, mobility of MANETs increases the rate of false positives in these systems. There have been few signature-based IDSs developed for MANETs and little research on signatures of attacks against MANETs. Updating attack signatures is an important problem for this approach. Some systems use promiscuous monitoring of wireless communications in the neighbourhood of nodes.

4.1 Zone-Based Intrusion Detection System

It is obvious that local detection alone cannot guarantee satisfactory performance because of limited security information obtained by each IDS agent. What's more, we may experience *alert flooding* problems given the distributed nature of MANETs. Therefore, a suitable framework is needed to integrate the alert information from a wider area. Moreover, attacks are likely to generate multiple related alerts. For example, because of the broadcast nature of radio channel, there may exist many victims suffering from same falsified routing control packets. The triggered alerts should have high correlations correspondingly. Therefore, it is desirable to treat them together. Based on the above considerations, we adopt a non-overlapping zone based framework. The whole network is divided into non overlapping zones. The formation and maintenance of zones are beyond the focus of this paper.



We assume the existence of such a framework. This could be done easily based on techniques like geographic partitioning [2]. As illustrated in figure, there are two categories of nodes in ZBIDS: intrazone nodes and *gateway* nodes (also called interzone nodes). If one node has a physical connection to a node in a different zone, this node is called a gateway node, for example, node 4, 7, 8 in the above figure. Otherwise, it is called an intrazone node. Only gateway nodes can generate *alarms*. They collect the local *alerts* broadcast from the intrazone nodes and perform aggregation and correlation tasks to suppress many falsified *alerts*. There may exist more than one

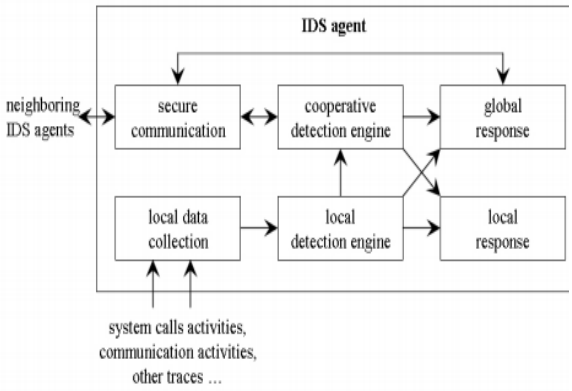
`

International Research Journal of Emerging Trends in Multidisciplinary
ISSN 2395-4434
Volume 1, Issue 5 July 2015
www.irjetm.com

gateway node in a single zone, all of which perform the alert aggregation task simultaneously. In this way, we can avoid the single point of failure. Note that in this paper, alerts and alarms have different meaning. Alerts indicate possible attacks and are generated by local IDS agents, while alarms indicate the final detection decision and can be generated only by gateway nodes [5].

4.2 Distributed and Cooperative IDS

Zhang and Lee also proposed the model for distributed and cooperative IDS as shown in Figure 2 [6]. The model for an IDS agent is structured into six modules. The local data collection module collects real-time audit data, which includes system and user activities within its radio range. This collected data will be analyzed by the local detection engine module for evidence of anomalies. If an anomaly is detected with strong evidence, the IDS agent can determine independently that the system is under attack and initiate a response through the local response module (i.e., alerting the local user) or the global response module



(i.e., deciding on an action), depending on the type of intrusion, the type of network protocols and applications, and the certainty of the evidence. If an anomaly is detected with weak or inconclusive evidence, the IDS agent can request the cooperation of neighboring IDS agents through a cooperative detection engine module, which communicates to other agents through a secure communication module [6].

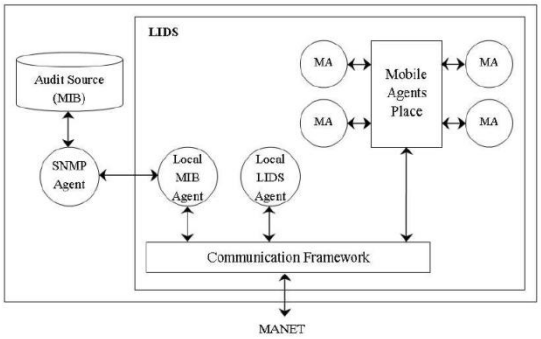
4.3 Local Intrusion Detection System (LIDS)

Albers *et al.* [5] proposed a distributed and collaborative architecture of IDS by using mobile agents. A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS. Two types of data are exchanged among LIDS: security data (to obtain complementary information from collaborating nodes) and intrusion alerts (to inform others of locally detected intrusion). In order to analyze the possible intrusion, data must be obtained from what the LIDS detect, along with additional information from other nodes. Other LIDS might be run on different operating systems or use data from different activities such as system, application, or network activities; therefore, the format of this raw data might be different, which makes it hard for LIDS to analyze. However, such difficulties can be solved by using SNMP (Simple Network Management Protocol) data located in MIBs (Management Information Base) as an audit data source [6]. Such a data source not only eliminates those difficulties, but also reduces the increase in using additional resources to collect audit data if an SNMP agent is already run on each node. To obtain additional information from other nodes, the authors proposed mobile agents to be used to transport SNMP requests to other nodes.

`

International Research Journal of Emerging Trends in Multidisciplinary
ISSN 2395-4434
Volume 1, Issue 5 July 2015
www.irjetm.com

In another words, to distribute the intrusion detection tasks. The idea differs from traditional SNMP in that the traditional approach transfers data to the requesting node for computation while this approach brings the code to the data on the requested node. This is motivated by the unreliability of UDP messages used in SNMP and the dynamic topology of MANETs. As a result, the amount of exchanged data is tremendously reduced. Each mobile agent can be assigned a specific task which will be achieved in an. The LIDS architecture is shown in figure, which consists of Communication Framework: To facilitate for both internal and external communication with a LIDS.



- Local LIDS Agent: To be responsible for local intrusion detection and local response. Also, it reacts to intrusion alerts sent from other nodes to protect itself against this intrusion.
- Local MIB Agent: To provide a means of collecting MIB variables for either mobile agents or the Local LIDS Agent. Local MIB Agent acts as an interface with SNMP agent, if SNMP exists and runs on the node, or with a tailor made agent developed specifically to allow updates and retrievals of the MIB variables used by intrusion detection, if none exists.
- Mobile Agents (MA): They are distributed from its LID to collect and process data on other nodes. The results from their evaluation are then either sent back to their LIDS or sent to another node for further investigation.
- Mobile Agents Place: To provide a security control to mobile agents. For the methodology of detection, Local IDS Agent can use either anomaly or misuse detection. However, the combination of two mechanisms will offer the better model. Once the local intrusion is detected, the LIDS initiate a response and inform the other nodes in the network. Upon receiving an alert, the LIDS can protect itself against the intrusion.

Conclusion

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 [7]. Accordingly, the study of the defense to such attacks should be explored as well. Many researchers are currently occupied in applying game theory for cooperation of nodes in MANETs [8, 9, 10, and 11] as nodes in the network represent some characteristics similar to social behavior of human in a community. That is, a node tries to maximize its benefit by choosing whether to cooperate in the network. There is not much work done in this area, therefore, it is an interesting topic for future research.

`

References

[1]Security Schemes for the OLSR Protocol for Ad Hoc Networks Daniele Raffo *PhD Thesis, University Paris 6 15 SEP 2005*

[2]M. Joa-Ng and I. Lu, "A Peer-to-Peer zone-based two-level link state routing for mobile Ad Hoc Networks," in IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, Aug., 1999, pp. 1415-1425

[3] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, \Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches,"*Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002)*, pp. 112, April 2002.

[4]B. Sun, K. Wu, and U. Pooch, "Routing Anomaly Detection in Mobile Ad-Hoc Networks," IEEE International Conference on Computer Communications and Networks (ICCCN'03), Dallas, TX, 2003, pp. 25-31.

[5] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, \Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," *Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002)*, pp. 112, April 2002.

[6]Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," the 6th Annual International Conf. on Mobile Computing and Networking (ACM MobiCom'00), Boston, MA, Aug., 2000, pp. 275-283.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, \Mitigating Routing Misbehavior in Mobile AdHoc Networks," *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00)*, pp. 255-265, August 2000.

[8] P. Michiardi and R. Molva, \A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad Hoc Networks,"*Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt'03)*, March 2003.

[9] A.Agah, S. K. Das, K. Basu, and M.Asadi, \Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach," *Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications (NCA'04)*, pp. 343-346, 2004.

[10] R. Mahajan, M. Rodrig, D. Wetherall and J. Zahorjan, \Experiences Applying Game Theory to System Design," *Proceedings of the ACMSIGCOMM Workshop on Practice and Theory of Incentives in Networked Systems (PIN'04)*, pp. 183-190, September 2004.

[11] S. Zhong, L. Li, Y. G. Liu and Y. Yang, \On Designing Incentive Compatible Routing and Forwarding Protocols in Wireless Ad-hoc Networks: An Integrated Approach Using Game Theoretical and Cryptographic Techniques," *Proceedings of the 11th Annual International Conference on Mobile Computing and Networking (MobiCom'05)*, pp.117-131, 2005.

`