Er. Banita Chadha , Dr. Ankit Chadha/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 1, Issue 3, pp.1203-1206

Intrusion Detection System in Mobile Adhoc NETworks:

Er. Banita Chadha[a] , Dr. Ankit Chadha[b]

[A] *Lecturer, Department of Information and Technology, Maharishi Markandeshwar Engineering College, Maharishi Markandeshwar University, Mullana, Ambala (Haryana).*
[B]*Proffesor, Department of Management and Technology, Maharishi Markandeshwar Management College, Maharishi Markandeshwar University, Mullana, Ambala (Haryana).*

ABSTRACT:
In recent years, the use of mobile ad hoc networks (MANETs) has been widespread in many applications, including some mission critical applications, and as such security has become one of the major concerns in MANETs. Additionally, the limited processing power and battery life of the devices used in a MANET also prevent the adoption of heavy-duty cryptographic techniques. While traditional misuse-based Intrusion Detection Systems (IDSes) may work in a MANET, watching for packet dropouts or unknown outsiders is difficult as both occur frequently in both malicious and non-malicious traffic. Mobile Ad-hoc Networks (MANETs) pose unique security requirements and challenges due to their reliance on open, peer-to-peer models that often don't require authentication between nodes. In this paper, we classify the architectures for intrusion detection systems (IDS) that have been introduced for MANETs. Current IDS's corresponding to those architectures are also reviewed and compared.

Keywords: Need for IDS, Architecture for Intrusion Detection System in MANET, IDS Mobile agent, IDS Activities, IDS Infrastructure.

1. INTRODUCTION

MANETs, or Mobile Ad-hoc NETworks, have recently gained adoption in a broad variety of environments thanks to improvements in wireless networking technology and the need for rapid mobile deployment. While the great flexibility of wireless ad hoc networks also brings many research challenges. One big issue is the security problem. Developing a practical application of wireless ad hoc network depends largely on the provided security level. However, recent researches
[1-3] indicate that the wireless ad hoc network is more vulnerable than the conventional wired and wireless networks due to its underlying characteristics of open medium, dynamic network topology, limited bandwidth , distributed cooperation and constrained energy resources. Several special properties lead to the uniqueness of MANET:

1) Wireless media is used for communication

2) Network topologies and memberships are constantly changing

3) No predefined trust exists between communication partners

4) Limited bandwidth, battery lifetime, and computation power prohibits the deployment of complex routing protocols or encryption algorithms

The Need for Intrusion Detection:

Intrusion prevention measures, such as encryption and authentication, can be used in ad-hoc networks to reduce intrusions, but cannot eliminate them. For example , encryption and authentication cannot defend against compromised mobile nodes, which often carry the private keys. The history of security research has taught us a valuable lesson no matter how many intrusion prevention measures are inserted in a network, there are always some weak links that one could exploit to break in (just like the example at the beginning of this paper). Intrusion detection presents a second wall of defence and it is a necessity in any high-survivability network. To secure mobile computing applications, we need to deploy intrusion detection and response techniques, and further research is necessary to adapt these techniques to the new environment, from their original applications in wired network. In this paper, we focus on a particular type of mobile computing environment called mobile ad-hoc networks and propose a new model for intrusion detection and response for this environment.

2. ARCHITECTURE FOR IDS IN MANETS:

Based on the network infrastructures, the MANET can be configured to either flat or multi-layer.
The optimal IDS architecture for the MANET may depend on the network infrastructure itself.
There are four main architectures on the network , as follows:

1) Standalone IDS,

2) Distributed and Collaborative IDS,

3) Hierarchical IDS, and

4) Mobile Agent for Intrusion Detection Systems.

The network architectures for MANET with regards to its applications are either flat or multi layer. Therefore optimum network architecture for a MANET depends on its infrastructure. In flat network infrastructures, all nodes are considered equal. Thus, they are suitable for applications such as virtual classes or conferences. In multilayer infrastructures, all nodes are considered different.

Stand-alone IDSs:

In this architecture, one IDS is executed independently for each node, and the necessary decision taken for that node is based on the data collected, because there is no interaction among network nodes and therefore no data is interchanged. In addition, each node has no knowledge of the position of other nodes in that network and no alert information crosses the network. Even though, due to its limitations, they are not effective, but they can be suitable for networks where nodes are not capable of executing an IDS or where an IDS has been installed.

Distributed and Cooperative IDSs

MANETs are distributed by nature and requires nodes cooperation. Zhang and Lee [5] put forward an intrusion detection system in MANET which is both distributed and dependent on nodes cooperation. Each node cooperates in intrusion detection and an action is performed by IDS agent on it. Each IDS agent is responsible for detection, data collection and local events in order to detect intrusions and generate an independent response.

Hierarchical IDSs

Hierarchical IDS architecture is the well developed distributed and cooperative IDS architecture and has been presented for multi-layered network infrastructure in such a way that network is divided into clusters. The cluster-heads of each cluster has more responsibilities compared to other members, For example, sending routing packets between clusters. In this way, these cluster-heads, behave just like control points, for example switches, routers or gateways, in wired networks. The name multi-layer IDS is also used for hierarchical IDS architecture.

Mobile Agent for IDSs

Mobile agents have been deployed in many techniques for IDSs in MANETs. Due to its ability of moving in network, each mobile agent is considered for performing just one special task and then one or more mobile agents are distributed amongst network nodes. This operation allows the distributed intrusion detection in the system. There are advantages for using mobile agents [6]. Some responsibilities are not delegated to every node, and so it helps in reducing the energy consumption, which is also an important factor in MANET network. It also provides for fault tolerance in such a way that if the network is segmented or some of the agents break down, they can still continue to function. Individual IDS agents are placed on each and every node. Each the IDS agent runs independently and monitors local activities (user and systems activities, and communication activities within the radio range). The agent detects intrusion from local traces and initiates response. If anomaly is detected in the local data, or if the evidence is inconclusive and a broader search is warranted, neighboring IDS agents will cooperatively participate in global intrusion detection actions. These individual IDS agents collectively form the IDS system to defend the wireless ad-hoc network.

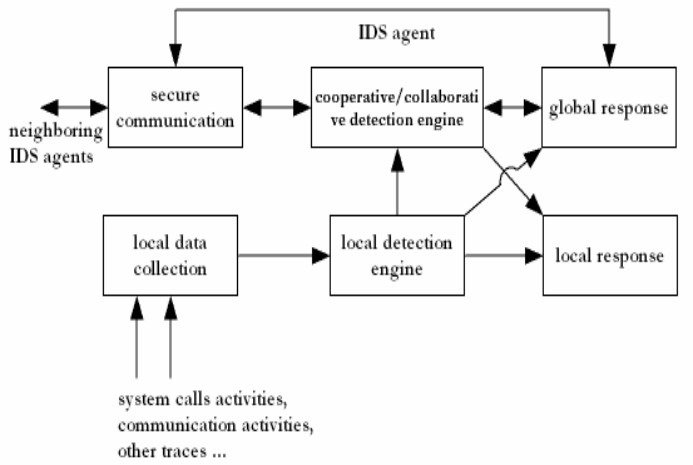
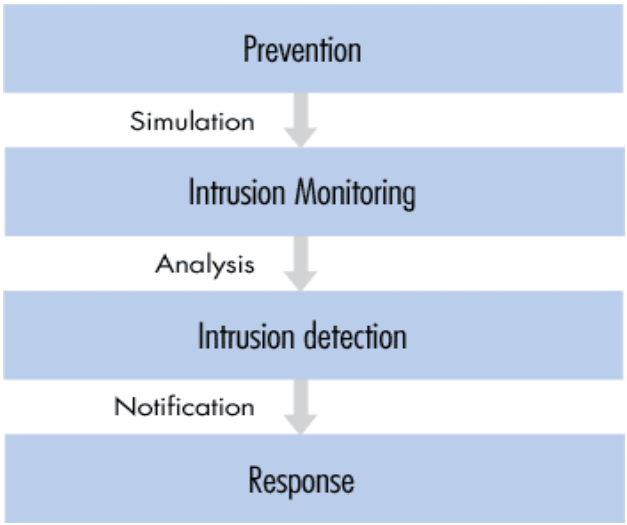


Figure 1) IDS Agent Model

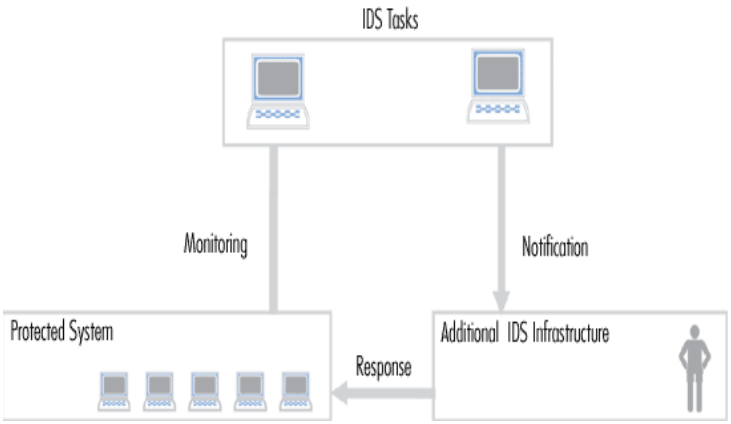
A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS. Two types of data are exchanged among LIDS: security data (to obtain complementary information from collaborating nodes) and intrusion alerts (to inform others of locally detected intrusion). In order to analyze the possible intrusion, data must be obtained from what the LIDS detects on, 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 Simple Network Management Protocol (SNMP) data located in Management Information Base (MIBs) as an audit data source. 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. 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 initiates a response and informs the other nodes in the network. Many intrusion detection systems have been proposed in traditional wired networks, where all trac must go through switches, routers, or gateways. Hence, IDS can be added to and implemented in these devices easily [7, 8]. On the other hand, MANETs do 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 unusual activities in a mobile environment. The network infrastructures that MANETs can be configured to are either at or multi-layer, depending on the applications. Therefore, the optimal IDS architecture for a MANET may depend on the network infrastructure itself [9]. In a °at network infrastructure, all nodes are considered equal, thus it may be suitable for applications such as virtual classrooms or conferences. Intrusion detection system serves as an alarm mechanism for a computer system. It detects the security comprises happened to a computer system and then issues an alarm message to an entity, such as a site security officer so that the entity can take some actions against the intrusion (Axelsson, 2000;Greg, 2004). In the discussion of IDS in MANET, two concepts need to be distinguished: intrusion detection techniques and intrusion detection architecture. Intrusion detection techniques refer to the concepts such as anomaly and misuse detection. They mainly solve the problems how an IDS detects an intrusion with a certain algorithm, given some audit data as input data. It can be viewed as an algorithm. The intrusion detection architecture, however, deals with problems in a larger scope. The intrusion detection technique is basically independent from the architecture or environment. In other words, anomaly and misuse detection can be utilized in wireless environment just as they are in wired network. The difference in implementation is mainly on what audit data to take as input to the algorithm. However, most IDS in MANET utilize anomaly detection because of the special nature of MANET. Intrusion detection may sometimes produce false alarms, for example as a result of malfunctioning network interface or sending attack description or signatures via email.

The main task of intrusion detection systems is defense of a computer system by detecting an attack and possibly repelling it. Detecting hostile attacks depends on the number and type of appropriate actions (Fig.1). Intrusion prevention requires a well-selected combination of “baiting and trapping” aimed at both investigations of threats. Diverting the intruder’s attention from protected resources is another task. Both the real system and a possible trap system are constantly monitored [5]. Data generated by intrusion detection systems is carefully examined (this is the main task of each IDS) for detection of possible attacks (intrusions).



(Fig.2) Intrusion detection system activities



(Fig.3) Intrusion detection system infrastructure

Once an intrusion has been detected, IDS issues alerts notifying administrators of this fact. The next step is undertaken either by the administrators or the IDS itself, by taking advantage of additional countermeasures (specific block functions to terminate sessions, backup systems, routing connections to a system trap, legal infrastructure etc.) – following the organization’s security policy (Fig.3). An IDS is an element of the security policy.[5]

Among various IDS tasks, intruder identification is one of the fundamental ones. It can be useful in the forensic research of incidents and installing appropriate patches to enable the detection of future attack attempts targeted on specific persons or resources.

3. CONCLUSION:

With the nature of mobile ad hoc networks, almost all of the intrusion detection systems (IDSs) are structured to be distributed and have a cooperative architecture. Ad hoc

networks are an increasingly promising area of research with lots of practical applications.

4. REFERENCES:

[1] Magazine, Vol. 13, No. 6, November/December 1999.

[2] F. Stajano and R. Anderson, "The Resurrecting Ducking: Security Issues for Ad-hoc Wireless Networks," Proceedings of the 7th International Workshop on Security Protocols, 1999.

[3] Lakshmi Venkatraman and Dharma P. Agrawal, "A Security Scheme for Routingin Adhoc Networks," Proceedings of the Wireless Communications and Networking Conference (WCNC), Vol. 3, pp. 1268-1273, 2000.

[4]Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks Gabriela F. Cretu, Janak J. Parekh, Ke Wang, Salvatore J. Stolfo Columbia University Department of Computer Science {gcretu, janak, kewang, sal}@cs.columbia.edu

[5] A Survey on MANET Intrusion Detection Satria Mandala satriamandala@hotmail.com
Faculty of Science & Technology Department of Informatics Engineering State Islamic University of Malang
Jl. Gajayana 50 Malang, Indonesia

[6] Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes
Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi

[7] Y. F. Jou, F. Gong, C. Sargor, X. Wu, S. Wu, H. Chang, and F. Wang,
\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.
[8] 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.

[9] Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks Gabriela F. Cretu, Janak J. Parekh, Ke Wang, Salvatore J. Stolfo Department of Computer Science Columbia University New York, US {gcretu, janak, kewang, sal}@cs.columbia.edu .

[10] A Survey on Intrusion Detection in Mobile Ad Hoc Networks Tiranuch Anantvalee *Department of Computer Science and Engineering Florida Atlantic University, Boca Raton, FL 33428*
E-mail: tanantva@fau.edu
Jie Wu *Department of Computer Science and Engineering Florida Atlantic University, Boca Raton, FL 33428*
E-mail: jie@cse.fau.edu

[11] Guidelines on Selecting Intrusion Detection Methods in MANET
Yi Li and June Wei
University of West Florida
Pensacola, Florida 32514, USA

[12] P. Brutch and C. Ko, \Challenges in Intrusion Detection for Wireless
Ad-hoc Networks," *Proceedings of 2003 Symposium on Applications and
the Internet Workshop*, pp. 368-373, January 2003.