Journal of Computer Applications Research and Development (JCARD), ISSN 2248 – 9304 (Print), ISSN 2248 – 9312 (Online), Volume 1, Number 1, April-June (2011)
pp. 01-07 © PRJ Publication
http://www.prjpublication.com/JCARD.asp

JCARD

© PRJ PUBLICATION

ESTIMATING DETECTION TRUST HOLD FOR INTRUSION DETECTION SYSTEMS IN MOBILE AD HOC NETWORK: A COMPREHENSIVE STUDY

M.B. Mukesh Krishnan[1] Prof. Dr. P. Sheik Abdul Khader[2]

[1] Research Scholar, Sathyabama University
Chennai 600 119, India
mukesh_krishnan@yahoo.com

[2] Professor and Head, Department of Computer Application
B.S. Abdur Rahman University, Vandalur,
Chennai-600 048,India
psaabdul@gmail.com

ABSTRACT

A mobile ad hoc network (MANET) is a self-configuring network without any basic infrastructure. Due to the characteristics of MANET, prevention from attack become more difficult and not sufficient to make them secure therefore, detection should be added as another defense before an attacker can breach the system. In general, the intrusion detection techniques will solve that purpose. Many Intrusion detection techniques as well as intrusion detection architecture for intrusion detection system (IDS) that have been introduced for Mobile ad hoc network (MANET).In this paper we make a study of MANET intrusion detection techniques as well as intrusion detection architecture and critically analysis the strength and limitation of each models then finally we estimate the detection trust hold of all models towards attack will be estimated through injecting sampling attacks towards common frame work to all models and analysis the detections done by them.

Keywords: mobile Ad Hoc networks, intrusion detection system (IDS), fault tolerance ,attack , intrusion detection technique, intrusion detection architecture

1. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network without any basic infrastructure each node is communicate through wireless transmitter and receiver with in the, radio communication range. In order to enable multi-hop communication notes act as host as well as router. The network topology frequently changes due to the mobility of mobile nodes as they move within, move into, or move out of the network. Initially MANET developed for military purposes, at present using for certain commercial uses where networks can be done without the help of any infrastructure or interaction with a human.

Security in MANET becoming a major issue when commercial uses of the network got into focus. Various solutions to prevent nodes from various attacks are proposed but prevention from

attack become more difficult and not sufficient to make them secure therefore, detection should be added as another defense before an attacker can breach the system. In general, the intrusion detection techniques will solve that purpose.

Intrusion detection can monitor activities in a system, collects activity information and then analyzes it to determine whether there are any activities that violate the security rules. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity. Although there are several intrusion detection techniques developed for today, those techniques should be reviewed and analyzed to enable the new techniques must which could be developed to make intrusion detection work effectively in MANET.

In this paper, we critically analysis the strength and weakness of IDS models and finally the estimate the detection trust hold of all IDS models towards attack.

2. INTRUSION DETECTION SYSTEM BACK GROUND

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. Intrusion detection architecture needs to employ certain intrusion detection techniques as a module. But it also contains many other modules, such as a module on how the nodes in a network can collaborate in intrusion detection decision making. In wired network, a node can usually make intrusion detection decision based on the data collected locally. Therefore, an intrusion detection technique can meet the need for intrusion detection once it is deployed on a node. In mobile network, however, it is very difficult for a node to make decision just based on data collected locally. Nodes must collaborate or exchange data at least in making an intrusion detection decision. Therefore, architecture to define the roles of different nodes and the way they communicate is extremely important in mobile IDS.

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 classiffed into three categories[2].

2.1. Anomaly detection systems: 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.

2.2 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.

2.3 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.

3. MANET INTRUSION DETECTION ARCHITECTURE

The MANET intrusion detection architecture are classified into three major types[3] based on the network infrastructure, configurations and decision making techniques as follows: 1. Stand-alone IDS, 2. Distributed and Cooperative IDS, 3. Hierarchical IDS,

3.1 Standalone IDS

In the stand alone architecture, the IDS runs on all nodes independently and the necessary decision taken for that node independently without cooperation or data exchange among other IDS present in the network 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 installed. This architecture is also more suitable for flat network infrastructure than for multi layered network infrastructure. This architecture is not effective enough but can be utilized in an environment where not all nodes are capable of running IDS.

3.2 Distributed and Cooperative IDS: In this architecture, each node has a IDS agent and make local detection decision. At the same time, all the nodes participate in a global detection decision making. This is more suitable to a flat MANET.

3.3 Hierarchical IDS: This architecture is designed for multi-layer MANET. In a multi-layered MANET, cluster-head (CH) nodes centralized routing for all nodes in the cluster and can support security measures including IDS. In addition, the CH nodes can also detect attacks against the virtual backbone's routing protocol made by Byzantine CH nodes, which is extremely important in MANET . Moreover, two types decision making for intrusion detection in MANET existing include collaborative decision making and independent decision making as follows: Collaborative and independent decision making

3.3.1 Collaborative decision making: Each node participates actively in the intrusion detection process. Once one node detects an intrusion with confidence high enough, this node can start a response to the intrusion. In a simple implementation of this design, a majority voting scheme is used to determine whether attack happens. This design can also use more complicated decision making schemes such as fuzzy logic. This design has some weak points in terms of security. It is more easily under the attacks such as denial of service and spoofed intrusion. In spoofed intrusion, a malicious node triggers full-forced intrusion response, which affects the whole network .

3.3.2 Independent decision making: In this framework, certain nodes are assigned for intrusion detection. These nodes collect intrusion alerts from other nodes and determine whether any node in the network is under attack. These nodes do not need other nodes' participation in decision making. This design also has weak points: in order to make a

good decision, the decision making node need collect a large amount of data from other nodes. However, such collection is very expensive in MANET, whose the network resources are especially limited.

4. ESTIMATING DETECTION TRUST HOLD FOR MANET INTRUSION DETECTION ARCHITECTURE

As a first step we analysis the various detection models and then we estimate the detection trust hold among them. As researchers produced various models for IDS ,we analysis the various architectures developed by them through the following as parameters

- Type of Architecture
- Node Cooperation
- Attacks Addressed
- Detection Technique Used
- Advantage of the Model
- Limitation of the Model

In 2007 G.A. Jacoby & N.J. Davis [5] proposed a standalone IDS architecture where node cooperation is low addressed the detecting malicious actions by comparing a node's power consumption with a set of power consumption patterns induced by known attacks, using smart battery technology which is more reliable and detects multiple attacks which holds a limitation of detects only attacks that cause power consumption irregularities.

In 2008 S.A. Razak, S.M. Furnell, N.L. Clarke, P.J. Brooke [9] proposed a Distributed and cooperative IDS where node cooperation is moderate which detects malicious actions using cooperative two-tier detection method where detection accuracy is high and false detection is low which needs trust evaluation to sustain towards attack.

In the same year 2008 N. Marchang, & R. Datta [11]proposed a hierarchical IDS with high node cooperation which act towards Routing Attacks using clustered structure to improve battery power through two layers of detection which holds the limitation such that high mobility will reduce the detection accuracy.

In 2009 Chuan-xiang Ma, & Ze-ming Fang [13] proposed a hierarchical IDS with high node cooperation which act towards malicious node through voting scheme to perform intrusion detection with low processing and communication overhead with a limitation that malicious nodes may exploit the detection scheme by voting legitimate nodes as malicious

In 2010 A. Lauf, R. A. Peters, & W. H. Robinson[7] proposed a standalone IDS where no cooperation between nodes, detects node misbehavior through two Stage detection method with two detection engine at each node where detection hypothesis is low.

The analysis shows us that each and every type of architecture will sustain to particular type of attack or environment we need to detect the detection trust hold among all the IDS architecture to state the effectiveness of the system towards all possible type attacks and environment.

Now as a second step we frame a common frame work to estimating detection trust hold among different models. Framework for the comparison study on intrusion detection in

MANET through seven stages. The detailed descriptions for each of these stages as follows

Input: up on the attack data to be collected by the IDS. It mainly includes system audit data, network packet or statistics of such data, for instance the statistics of updates in routing table.
Clustering nodes: certain algorithms are run on the network so that the network is partitioned into a number of clusters. A cluster usually has a node as the cluster head. The network partition and cluster head selection is dynamic.

Local detection: The IDS module or agent on a single node run intrusion detection algorithm to determine whether intrusion happens on the local node. Get information from other nodes: This usually happens on cluster head. Because of the distributed and ad hoc nature of MANET, the local information on a single node is often insufficient for detection decision making. Therefore, the IDS need to collect information from other nodes rather than the node it resides in to make accurate detection.

Independent detection decision making: The IDS on the cluster head make intrusion decision with all the information it acquires.

Collaborative detection decision making: Several nodes participate in a collaborative decision making process, for instance a voting to make the intrusion decision. Usually, before the voting, each of the participating nodes already makes an initial decision. They need to aggregate the initial decisions to make a more accurate group decision.

Communication Mechanism: Several communication scenario are used along with the Agent, cluster and mobility for the nodes.

Output : One of the most important problems facing proposed IDS in MANET is the high ratio of false alarms. The testing team must consider this measurement in order to determine the rate of the false-positives generated during a specific scenario

The estimation carried out for all the identified models towards detecting detection trust hold among the IDS architecture by providing a common input by injecting attacks into a stream that penetrates through various environment to detect intruders and summarized in table 1.

Model Authors	Input	Clustering nodes	Local detection	Independent detection decision making	Collaborative detection decision making	Communication Mechanism	Output
G.A. Jacoby & N.J. Davis	Locally audit data	No	Yes	Yes	No	Standalone	High ratio of false alarm
S.A. Razak, S.M. Furnell, N.L. Clarke, P.J. Brooke	Audit data and Network statistics data	Yes	Yes	No	Yes	Distributed	False alarm ratio is moderate
N. Marchang, & R. Datta	Audit data and Network statistics data	Yes	Yes	No	Yes	hierarchical	False alarm ratio is moderate
Chuan-xiang Ma, & Ze-ming	Audit data and Network statistics data	Yes	Yes	No	Yes	hierarchical	False alarm ratio is moderate
Lauf, R. A. Peters, & W. H. Robinson	Locally audit data	No	Yes	Yes	No	Standalone	High ratio of false alarm

The table shows that clustering and decision making should join the hand with local detection to reduce the ratio of false detection . In addition, many of them are vulnerable to security attacks, which might: hinder the network operation and the intrusion detection process, mislead detection, or falsely characterize legitimate nodes as malicious. Finally, evaluated IDS architectures cannot detect all types of attacks, since they focus only on specific types of intrusions.

5. CONCLUSION AND FUTURE DIRECTIONS

Intrusion detection techniques act as a defense to safeguard the node from attacks. In this paper we studied and analyzed various intrusion detection architecture their strength and limitation are estimated finally we estimated the detection trust hold of all models towards attack through injecting sampling attacks towards common frame work to all models and analysis the detections done by them and the result we found that detection trust hold is weak all the models as well as each and every model focus on specific type of intrusions to be detected so we need a IDS architecture which should avoid false detection and mislead detection with the ability of detecting all type of intruders inside the environment.

6. REFERENCES

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

[2].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.

[3]. T. Anantvalee and 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)

[4]. Y. Xiao, X. Shen, and D.Z. Du, *Wireless/Mobile Network Security,* Springer, 2006. Ch.7.

[5] G.A. Jacoby, N.J. Davis, "Mobile Host-Based intrusion Detection and Attack Identification," IEEE Wireless Communications, vol. 14, issue 4, pp. 53-60, August 2007.

[6] K. Nadkarni, A. Mishra, "A Novel Intrusion Detection Approach for Wireless Ad Hoc Networks," IEEE Wireless Communications and Networking Conference (WCNC. 2004), vol. 2, pp. 831 – 836, March 2004.

[7] A. Lauf, R. A. Peters, W. H. Robinson, "A Distributed Intrusion Detection System for Resource-Constrained Devices in Ad Hoc Networks". Elsevier Journal of Ad Hoc Networks, vol. 8, issue 3, pp. 253-266, May 2010.

[8] W. Wang, H. Man, Y. Liu, "A Framework for Intrusion Detection Systems by Social Network Analysis Methods in Ad Hoc Networks." Wiley Security and Communication Networks, vol. 2, issue 6, pp. 669 – 685, April, 2009.

[9] S.A. Razak, S.M. Furnell, N.L. Clarke, P.J. Brooke, "Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks," Elsevier Ad Hoc Networks, vol. 6, issue 7,pp. 1151 – 1167, September 2008.

[10] C. Ramachandran, S. Misra, M. Obaidat, "FORK: A novel two-pronged strategy for an agentbased intrusion detection scheme in ad-hoc networks," Elsevier Computer Communications, vol. 31, issue 16, Performance Evaluation of Communication Networks (SPECTS 2007), pp. 3855-3869, October 2008.

[11] N. Marchang, R. Datta, "Collaborative techniques for intrusion detection in mobile ad hoc networks," Elsevier Ad Hoc Networks, vol. 6, issue 4, pp. 508 – 523, June 2008.

[12] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, P. Bhattacharya, "A game-theoretic intrusion detection model for mobile ad hoc networks," Elsevier Computer Communications vol. 31, issue 4, pp. 708-721, March 2008.

[13] Chuan-xiang Ma, Ze-ming Fang, "A novel intrusion detection architecture based on adaptive selection event triggering for mobile ad-hoc networks," IEEE Second International Symposium on Intelligent Information Technology and Security Informatics, pp.198-201, January 2009.