ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

# Comparative Study of Various Distributed Intrusion Detection Systems for WLAN

[I]Davinder Singh, [II]Mohd. Ibraheem Shah, [III]Vishwa Pratap Singh
[I,II,III]Kamal Institute of Higher Education and advance Technologies, K-1 Extn, Mohan Garden, New Delhi, India

**Abstract**
*In any information system intrusions are the activities that damage the security and integrity of the system. In this paper we focus on wireless network, intrusions in wireless network (WLAN) and different Distributed Intrusion Detection Systems which are used to detect these attacks or intrusions. The rapid enhancement in wireless network has changed the level of network security. So, past of protecting the network with the firewalls are not sufficient to maintain network security in wireless local area network. There are different intrusion detection techniques which are used for identifying the various types of intrusions in wireless local area network. In this paper, we compare the various Distributed intrusion detection Systems used for detecting attacks in wireless network and also make a comparison table of these DIDS depending upon the performance. This comparison table will very helpful in designing better intrusion detection systems for detecting and preventing of vulnerabilities in wireless network.*

**Keywords**
*Networks, Intrusions, IDS, Intrusion Detection Systems, DIDS, Comparison, DDOS, Wlan*

## I. Introduction

Wireless networks are becoming so popular for many applications because they provide communication between different systems without predetermined infrastructure. Due to this flexibility new security risks are introduced in wireless network. The wireless network is dynamic in nature so there are number of challenges in maintaining security in wireless network. In wireless network there is need of defense schemes which are stronger, efficient and flexible. Intrusions in an information system are the processes or activities that damage the security policy of system. Intrusion detection is the process detecting and reporting unauthorized or unapproved network activity. It is used to identify intrusions or attacks against the system. Intrusion detection system (IDSs) collects and scrutinizes the data to recognize computer system and network intrusions or mishandlings. Conventional IDSs have been designed for wired systems and networks to identify intrusions or attacks. Of late, wireless network have been concentrated for employing the IDSs Constructed. Monitoring, analyzing user and system activities, identifying abnormal network activities and detecting policy violations for WLANs are the functions of these wireless IDSs. There are a lot of chances of attacks in WLANs due to dynamic topology, absence of infrastructure and centralized administration. Wireless IDSs collect all local wireless transmissions and rely either on predefined signatures [1] or on anomalies in the traffic [3] to produce alerts or alarms. In this paper we focus on different types of attack in wireless network, various distributed intrusion detection systems, research achievements in DIDSs fields and their comparison. Ease of Use.

## II. Vulnerabilities in Wireless

Finally In wired network data travel from one place to another over a dedicated physical line that is private, but in WLAN data travel from one place to another over a shared space which is not private. It means there are more chances of vulnerabilities in wireless networks as compare to wired networks. Wireless networks have characteristics like dynamic topology, absence of centralized administration and low protection of nodes. Due to dynamic topology nature of wireless network there is no boundary of wireless network, so old methods like firewall protection are not applicable for security in WLAN. Different types of vulnerabilities in WLAN are:

### A. Due to lack of infrastructure

In wireless networks there is no fixed infrastructure which makes different security mechanism inapplicable like certification, firewall and cryptography.

### B. Vulnerability due to channels

In wireless network fake messages can easily be injected without making physical connection with the network.

### C. Dynamic topology

In wireless networks dynamic topology is used which require sophisticated routing protocols. Problem arises due to mobility of devices. It is very difficult to track a misbehaving device in wireless network which generate wrong routing information.

### D. Vulnerability due to nodes

In wireless network it is not possible to protect the different nodes physically. That is why these nodes can easily be captured by an attacker.

## III. Classification of Intrusion Detection System

Intrusion Detection Systems (IDSs) are the software designed for detecting, blocking and reporting unauthorized activities in computer networks. An Intrusion Detection System (IDS) can be categorized into two different forms according to data collection mechanisms and attack detecting techniques [4] as shown in fig.1.

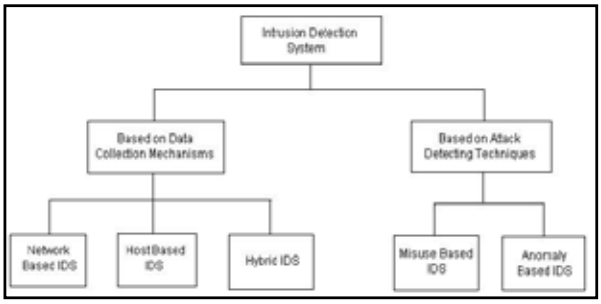


Fig.1.Classification of Intrusion Detection System.


© All Rights Reserved, IJARCST 2014

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

### A. Based on Data Collection Mechanism

Define IDS can be categorized into three types [6] according to the data collection method: Network Based, Host Based, Hybrid intrusion detection system. Network based intrusion detection system reside on a separate system from where it watches the network traffic, looks for indications of attacks that traverse the portion of the network. Host based intrusion detection system resides on a particular host and looks for the indications of attacks on that host. Hybrid intrusion detection system has both the functionality of Network based and Host based intrusion detection system.

### B. Network Based IDS

Network Based IDS (NIDS) exists as a software process on a dedicated hardware. The NIDS places the network interface card on the system into promiscuous mode, i.e. the card passes all traffic on the network to the NIDS software. The traffic is then analyzed according to a set of rules and attack signatures to determine if it is traffic of interest. If it is, an event is generated. Its attack recognition module uses four common techniques to recognize an attack signature:

- Pattern, expression or byte code matching,
- Frequency or threshold crossing
- Correlation of lesser events
- Statistical anomaly detection

Once an attack has been detected, the IDS' response module provides a variety of options to notify, alert and take action in response to the attack. Problem with NIDS is that it has high false positive rate. Another drawback is that in NIDS there is no central point to monitor whole N/W. So, it is not good for adhoc network.

### C. Host-Based IDS

HIDS exists as a software process on a system. HIDS examines log entries for specific information. Periodically, the HIDS process looks for new log entries and matches them up to pre-configured rules. If a log entry matches a rule, the HIDS will alarm. Today's host-based intrusion detection systems remain a powerful tool for understanding previous attacks and determining proper methods to defeat their future application. Host-based IDS still use audit logs, but they are much more automated, having evolved sophisticated and responsive detection techniques.

### D. Hybrid IDS

Hybrid intrusion detection system is an IDS which combine the functionality of network based sensor technology with host based agent that is capable of analyzing the network traffic only addressed to specific host where agent of hybrid IDS is installed [8].

- Based on Detection Techniques
  An intrusion detection system can be categorized into two different forms based on detection techniques: Signature or Misuse based and Anomaly based intrusion detection system.
- Signature or Misuse based IDS
  Misuse detection attempts to model abnormal behavior or signatures of known attacks. It is based on the assumption that all intrusions or attacks leave their signatures that can be detected[9,10]. Any occurrence of which clearly indicates system abuse. For Example, an HTTP request referring to the cmd.exe file may indicate an attack.
- Anomaly based IDS
  Anomaly based IDS attempts to model normal behavior. Events that violate this model are considered to be suspicious. For Example, a normally passive public web server attempting to open connections to a large number of addresses may be indicative of a worm infection.Equations

## IV. Vulnerabilities in Wireless

Depending upon the infrastructure the wireless network can be divided into two different forms either flat or multi-layer. The best architecture of IDS for a wireless network depends upon the infrastructure of that network. The different types of IDS architecture are:

### E. Standalone Architecture

In this type of architecture Intrusion Detection System (IDS) runs on each system to find out intrusions independently. In standalone architecture there is no data exchange and no cooperation among IDSs on the network. This architecture is more appropriate for network with flat infrastructure than for network with multilayered infrastructure [13].

### F. Distributed and Collaborative Architecture

In this type of architecture every node in wireless network takes part in intrusion detection process with the help of IDS agent running on the different nodes. In distributed and collaborative architecture IDS agent is responsible for collecting and detecting the local events and data to find out different intrusions or attacks .After identifying the intrusion IDS give response at the same time [14].

### G. Hierarchical Architecture

This architecture is the improved version of distributed and collaborative architecture. Hierarchical architecture is well suited for infrastructure of multi-layered network. In multi layered infrastructure network is divided into clusters and cluster heads in this type of infrastructure act as control points in the same way as routers, switches and gates in wired network [15].

### H. Architecture based on mobile agent

In this type of IDS architecture mobile agents are used to perform required task on different nodes in wireless network. In mobile agent based architecture distribution of attack detection tasks are possible. It is very best method of using mobile agents [16, 18] for detecting intrusions.

## V. Comparison of Different Distributed Intrusion Detection Systems

There are a lot of advantages and disadvantages of different distributed intrusion detection systems. Different distributed intrusion detection systems and there references are shown in table 1 and comparison of these systems is shown in table 2.

Table 1:

| Reference of Ids | Author | Algorithm | Merits | Demerits | ID Method |
|---|---|---|---|---|---|
| IDS1 | Kachirski and Guha | Mobile Agent Based | better network performance | Only use anomaly based method | Anomaly based |
| IDS2 | Y. Huang | Cluster based distrib-uted intrusion detection scheme | improved efficiency in the terms of network overhead and memory usage | false alarm rates are not mentioned and low perfor-mance | Anomaly based |

© 2014, IJARCST All Rights Reserved

| | | | | | |
|---|---|---|---|---|---|
| IDS3 | R. Puttini | A fully distributed algorithm | identify the source of packet dropping attack and suitable for manet | ery time consuming process to learn program profiles and testing processes | signature based |
| IDS4 | R. Nakkeeran | agent based cooperative and distributed system | low false alarm rate and performance is better than other ids | No description about security issuses of mobile agents | Anomaly based |
| IDS5 | Jelena Mirkovic | a distributed system for ddos defense | ability to detect new attacks and latest misuse signatures | faces some challenges like arbitrary definition of abnormal activities | signature based |
| IDS6 | James Cannady and Jay Harrell | cluster based intrusion detection system | reduces communication overheads and good detection rate | more complex and ineffective co-ordination between dids modules | Anomaly based |

## VI. Conclusion and Future Work

Only intrusion detection and prevention techniques are not sufficient for securing wireless network but there is also need of good Intrusion Detection System. From the existing DIDS anomaly based intrusion detection systems are more efficient and economic because of distributed nature of wireless ad hoc network. For better understanding of Distributed Intrusion Detection System we have given details of different DIDS. We have also given comparison table of different DIDS according to their performance. Future work will involve developing more intelligent and robust intrusion detection algorithms. We will investigate number of attacks on Intrusion Detection System infrastructure.

## References

[1] *Jatinder Singh, Dr. Lakhwinder Kaur & Dr. Savita Gupta, "Analysis of Intrusion Detection Tools for Wireless Local Area Networks," IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009. Pp. 169-176*

[2] *I.S. Jacobs and C.P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.*

[3] *K. Elissa, "Title of paper if known," unpublished.*

[4] *Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1988.*

[5] *M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.*

[6] *Herve Debar, "An Introduction to Intrusion-Detection Systems" IBM Research, Zurich Research Laboratory.*

[7] *Ning, P., Jajodia, S., & Wang, X.S. (2001). Abstraction-based intrusion detection in distributed environments. ACM Transactions on Information and System Security, 4 (4), 407--452.*

[8] *T. S. Sobh "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art", Computer Standards & Interfaces 28, pp. 670-694, Science Direct, 2006.*

[9] *P.G. Neumann and P.A. Porras, "Experience with EMERALD to date", in Proc. Workshop Intrusion Detection Network Monitoring, santa Clara, CA, Apr. 1999.*

[10] *Madge,(2005). Wireless Intrusion Detection System (ids) evolve to 3rd generation proactive protection systems. Retrieved Apr. 06, 2006, from http://www.telecomweb.com/ readingroom/Wi*

[11] *AikateriniMitrokotsa, Rosa Mavropodi, Christos Douligeris,"Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Network" TAyia Napa, Cyprus, July 6-7, 2006.*

[12] *Snapp, S.R., et al. (1991). DIDS (distributed intrusion detection system) ---Motivation, architecture, and an early prototype. In Proceedings of 14th national computer security conference (pp. 167--176).*

[13] *Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah, "A Survey on MANET Intrusion Detection", in: International Journal of Computer Science and Security, Volume (2) : Issue (1).*

[14] *Yian Huang, Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pages 135147, Fairfax, Virginia, 2003. ACM Press.*

[15] *O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks" Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03), p. 57.1,January 2003.*

[16] *R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai,"SAgent Based Efficient Anomaly Intrusion Detection System in Adhoc networks",IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.*

[17] *Sampathkumar Veeraraghavan, S. Bose, K. Anand and A. Kannan, "SAn Intelligent Agent Based Approach for Intrusion Detection and Prevention in Adhoc Networks",IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007.*

[18] *Yongguang Zhang,Wenke Lee,Yian Huang, "Intrusion Detection Techniques for Mobile Wireless Networks",Appear in ACM WINET Journal in 2003.*

[19] *Jelena Mirkovic, Max Robinson, Peter Reiher, George Oikonomou, " Distributed Defense Against DDoS Attacks", Technical Report CIS-TR-2005-02,CIS Department, University of Delaware,2005.*

## Author Profile

*Vishwa Pratap Singh received the B. Tech. Degree in Information technology and M.Tech degree from Indian Institute of Information technology in Computer science specialized in information Security. He is working as Assistant Professor in Computer Science department at Kamal Institute of Higher Education and advance technologies, Delhi. His main research area is information security, wireless sensor networks and system penetration testing.*


© All Rights Reserved, IJARCST 2014