ISSN 2229-5518

Survey on Intrusion Detection and Prevention System: A MANET Perspective

Abhishek Kundu, Tamal Kumar Kundu, I Mukhopadhyay

Abstract— These Recent computer systems are affected by viruses and malware. There are many techniques via which networks can be secured like encryption, firewalls, DMZ etc. Intrusion Detection System (IDS) is a type of system which detects attacks and notifies the same. Intrusion Prevention System (IPS) detects the attack and then prevents the system from further attacks. In recent times we have merge these two types of systems and rechristened it as Intrusion Detection and Prevention System (IDPS) the new system will simultaneously detect and prevent malicious activities. In recent years, the security issues on MANET have also become one more vulnerable area other than wired network. This paper presents a brief idea on the attacks and subsequently their respective preventive actions. Artificial Neural Networks is one type of architecture which can be used to design the hardware circuit for the same.

Index Terms—Intrusion Detection System, Intrusion Prevention System, MANET, Security

1 INTRODUCTION

Internet facility is truly ubiquitous now facilitate our society all over the world. Intrusion Detection System is that type of technique which detects malwares which have the capability to cause harm. But nowadays only detecting those malware is not enough we have to also recover from it. An Intrusion Prevention System (IPS) is software that has the capabilities of an intrusion detection system and can also attempt to stop possible incidents. There are four fundamental pillars of security are CAIA means Confidentiality, Authenticity, Integrity and Availability [1]. The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message. Authentications mechanisms help establish proof of identities. The authentication process ensures that the origin of an electronic message or document is currently identified. Integrity assures that the data received are exactly as same by an authorize entity [2]. The principle of availability states that resources should be available to authorize parties at all times. Apart from those pillars, there is another one, non-repudiation. It states that it provide protection against denials by one of the entity involved in a communication of having participated in all parts of the communication. Attacks is an assault on system security that derives from an intelligent threat i.e. an intelligent act i.e. a delivery attempt to event security services and violent the security policy of a system. There are two types of attacks (i) passive attacks and (ii) active attacks. Passive attacks are those, wherein attackers aims to obtain Information that is in transit. The term passive indicates that the attacker does not attempt to perform any modification to the data. In fact, this is also why passive attacks are harder to detect. The active attacks are based on modification of the original message in some manner or the creation of a false message [3]. Different methods are used to make a shield to protect a system. Cryptography is the first method to concealing the ensure data and the methods are RSA algorithm, DES and Diffiehellman algorithm etc. Another technique is Firewall to protect our system both software and hardware perspective [2]. In spite of all types of protection, the current scenario is so much complex that it requires higher systems to prevent malwares. Intrusion Detection System (IDS) is more fast and accurate and has articulated all types of problems in the system. And also Intrusion prevention System (IPS) is essential to detect security breaches. An intrusion detection system (IDS) is designed to monitor all inbound and outbound network activity and to identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. IPS or intrusion prevention system is definitely the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets. It provides policies and rules for network traffic along with IDS for alerting system or network administrators to suspicious traffic, but allows the administrator to provide the action upon being alerted. Where IDS informs of a potential attack, an IPS makes attempts to stop it. On the other hand a Mobile Ad Hoc Network is an independent system of mobile stations connected by wireless link to form a network. It is also known as infrastructure less, network because it does not trust on predefined infrastructure to keep the network connected. In MANET each node can exchange information with node in its range and those which are beyond the range can share information using the concept of multi hop communication in which other node receive and transmit the packet. Several routing protocols have been proposed for MANET and most popular are DSR, OLSR, DSDV, and AODV. Malicious nodes could exploit the weakness MANET to launch various kinds of attack. The characteristics of MANET like dynamic topology, lack of fixed infrastructure ,vulnerability of nodes and communication channel, lack of traffic concentration points, limited power computational capacity, memory and bandwidth make the task of achieving a secure and reliable communication more difficult [3]. Attacks like sleep deprivation, jamming transmission channel with garbage packets, black hole, warm whole, grey hole, DOS etc [5].

2 IDPS COMPONENTS

This section describes the major components of IDPS solutions and illustrates the most common network architectures for these components.

i. Sensor or Agent: Sensors and agents monitor and analyze activity. The term sensor is typically used for IDPSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term agent is typically used for host-based IDPS technologies.
ii. Management Server: A management server is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as correlation. Management servers are available as both appliance and software-only products. Some small IDPS deployments do not use any management servers, but most IDPS deployments do. In larger IDPS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.
iii. Database Server: A database server is a repository for event information recorded by sensors, agents, and/or management servers. Many IDPSs provide support for database servers [6].
iv. Console. A console is a program that provides an interface for the IDPS's users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDPS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDPS consoles provide both administration and monitoring capabilities [6].

2.1 Types of IDPS

The main four types of IDPS technologies-network based, wireless, NBA and host based

i. Network based IDPS: A network based IDPS (NIDPS) monitors wired networks traffic for particular Network segments or devices and analyses network, transport and application protocols to identify suspicious activity. Most of analysis is done in application layer. Transport and network layers also analyzed to identify attacks at those layers and to help the analysis in application layer [11].

Components and architecture: A typical networks- based IDPS includes all the basic components of IDPS. Figure 1 shows the architecture of NIDPS. Whenever feasible, those components should be connected through a management network. The sensors to be used with NIDPS solutions are equipped with network placed into promiscuous mode, which allows them to accept all packets, regardless of their intended destination. Sensors are available in two formats, appliance and software only [6]. An application based sensors is a piece of specialized hardware which comprises NIC's optimized for efficient capture of traffic; it also includes specialized processors or other hardware components that assist its analysis, as well as sensor software, which might reside its firmware for increased efficiency. A software-only sensor is a piece of

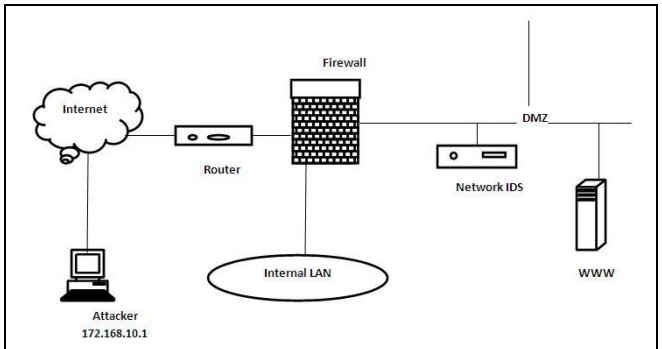

Fig. 1. Network based IDPS Architecture

software which is intended for use with normal hosts, provided that they meet certain requirements. Sensors can be deployed one in two modes: inline and passive mode. Choice increased the prevention capabilities of IDPS solutions. We are discussing this in below:

Inline Sensor: An inline sensor is located so that the network traffic it is intended to monitor must pass through it .The main reason for deploying inline sensor is to enable them to stop attack from outside by blocking traffic .They are usually placed where the firewall and other network security would be placed i.e. at the boundaries between networks. Some inline sensors may be integrated into an existing firewall device. For example, if a firewall is present between boundary and external and an internal network, the sensor should be placed internal side.

Passive Sensors: A passive sensor, on the other hand, is deployed in such a way as to monitor a copy of the network traffic, but no traffic actually passes through it. Passive sensors may be used to monitor key network segment such as activity on a demilitarized zone (DMZ). Network based IDPS typically make use of a combination of the three detection techniques. These are signature based, anomaly based and stateful protocol analysis. For example, stateful protocol analysis might be decomposing traffic into request response pairs and each of them may be examined for anomalies and compared to signatures [7].

ii. Host based IDPS: Host-based intrusion prevention systems are used to protect both servers and workstations through software that runs between your system's applications and OS kernel. The software is preconfigured to determine the protection rules based on intrusion and attack signatures. The HIPS will catch suspicious activity on the system and then, depending on the predefined rules, it will either block or allow the event to happen. HIPS monitors activities such as application or data requests, network connection attempts, and read or

write attempts to name a few [4]. A host-based IDPS could for example monitor incoming and outgoing wired and wireless network traffic system logs, running processes, file access and modification system and application configuration changes. The same kind of monitoring is often provided by a number of anti-virus software and personal firewall solutions. The distinction between these tools becomes very blurred, as many of them overlap in functionality [7].

iii. Network Behaviour Analysis (NBA): A flow is a particular communication session occurring between hosts. A Network Behaviour Analysis (NBA) system examines network traffic or statistics on network traffic identify unusual flow, such as distributed denial of service attacks, certain forms of malware and policy violations. The difference with a network-based IDPS solution does not seem striking: they serve much the same purposes, with NBA systems making broader use of anomaly-based techniques. NBA solution has some sensors and consoles; some products also include management server, which are sometimes calls analyzers [4].Sensors usually come in the form of appliances. NBA technologies can detect several types of malicious activity. Most of them use primarily anomaly-based detection, along with some stateful protocol analysis techniques; signature-based detection is usually not available [6]. The types of threat that can be identified include: denial of service attacks, by noticing significantly increased bandwidth usage or unusual data flows to/from specific hosts; scanning which generates a typical flow patterns.

iv. Hybrid IDPS: Both host based and network based are used articulately .A hybrid IDPS combines of HIDS, which monitors events occurring on the host system, with a NIDS [6], which monitors network traffic. On those upper contexts, we discuss on the IDPS components and their types. Now, we have to discuss what those techniques which are used in IDPS technologies are and how to bring them in our market. First we analyze on artificial neural networks which is designed by VHDL with the help of Xilinx ISE. Before started on this topic, we have to introduce some others techniques [4].

2.2 Techniques of Intrusion Detection

Many of the techniques are used to detect and prevent intrusion. IDPS technologies follow many types of methods to detect incidents. These methods are signature based technologies, anomaly based technologies, stateful protocol analysis and Behavioral analysis. Most IDPS technologies use multiple detection methodologies for their own purpose [8].

i. Signature Based Detection: Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats. For example, if an attacker modified the malware in the previous example to use a filename of "freepics2.exe" [6], a signature looking for "freepics.exe" would not match it.

ii. Anomaly Based Detection: Anomaly based detection is the considered normal against observed events to identify significant deviations. An IDPS using anomaly-based detection has profiles that represent the normal behavior of such things as users, hosts, network connections, or applications. The profiles are developed by monitoring the characteristics of typical activity over a period of time. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats. Anomaly based schemes fall into three main categories:
   a. Behavioral analysis: looks for anomalies in the types of behavior that have been statistically base lined, such as relationships in packets and what is being sent over a network [11].
   b. Traffic-pattern analysis: looks for specific patterns in network traffic. Protocol analysis looks for network protocol violations or misuse based on RFC-based behavior.
   c. Protocol analysis: has the benefit of identifying possible attacks that are not yet publicized or that there is no known signature or remedy for .But in this survey we discussed separately. Third technique of detection is stateful protocol analysis.

3 Related works for IDPS

Simply put, anomaly-based intrusion detection triggers an alarm on the IDS when some type of unusual behavior occurs on the network. This would include any event, state, content, or behavior that is considered to be abnormal by a pre-defined standard. Anything that deviates from this baseline of normal behavior will be flagged and logged as anomalous [7]. Normal behavior can be programmed into the system based on offline learning and research or the system can learn the. Some examples of anomalous behavior include:

i. HTTP traffic on a non-standard port, say port 53 (protocol anomaly)
ii. Backdoor service on well-known standard port, e.g., peer-to-peer file sharing using Gnutella on port 80 (protocol anomaly and statistical anomaly)
iii. A segment of binary code in a user password (application anomaly)
iv. Too much UDP compared to TCP traffic.(statistical anomaly)
v. A greater number of bytes coming from an HTTP browser than are going to it (application and statistical anomaly) [6].

4 Attack in MANET

The MANET is susceptible to passive and active attacks. The Passive attacks typically involve only eavesdropping of data, whereas the active attacks involve actions performed by adversaries such as replication, modification and deletion of exchanged data. In particular, attacks in MANET [3] can cause

congestion, propagate incorrect routing information, prevent services from working properly or shutdown them completely. Nodes that perform the active attacks are considered to be malicious, and referred to as compromised; while nodes that just drop the packets they receive with the aim of saving battery life are considered to be selfish [4]. A selfish node does not participate in the routing protocols and also not forwarding packets in the network. A compromised node may use the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept as in the so called black hole attacks.

5 IDS ARCHITECTURE IN MANET

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. In multilayer infrastructures, all nodes are considered different. Nodes may be grouped in clusters, with a cluster-head node for each cluster. To communication into a cluster, nodes are in direct contact with each other. Nodes communication between clusters is performed through each cluster-head nodes.

i. 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 [9]. This architecture is also more suitable for flat network infrastructure than for multi layered network infrastructure. Due to the fact that exclusive node information is not enough to detect intrusions, thus this architecture has not selected in many of the IDS for MANETs.
ii. Distributed and Cooperative IDSs: MANETs are distributed by nature and requires nodes cooperation. Zhang and Lee 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 [5]. This architecture, which is similar to stand-alone IDS architecture, is more suitable for flat network infrastructure compared with multi-level infrastructure [9].
iii. 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 [3]. The name multi-layer IDS is also used for hierarchical IDS architecture. Each IDS agent is performed on every member node and locally responsible for its node. Each cluster-head is locally in charge of its node and globally in charge of its cluster.
iv. Mobile Agent for IDSs: The mobile agent for IDS architecture uses mobile agents to perform specific task on a nodes behalf the owner of the agents [5]. This architecture allows the distribution of the intrusion detection tasksThe MANET is susceptible to passive and active attacks. The Passive

6 RELATED WORKS IN MANET

Wireless mobile network configuration depends on its application. The IDS architecture for a wireless mobile network should be designed based on the network infrastructure itself which can be flat or multi layered where node may be separated into different clusters each having a cluster head to allow communication process.

i. Distributed and Cooperative IDS: Zhang and Lee proposed the model for distributed and cooperative IDS as shown in Figure 1.The model for 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 [3]. 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.

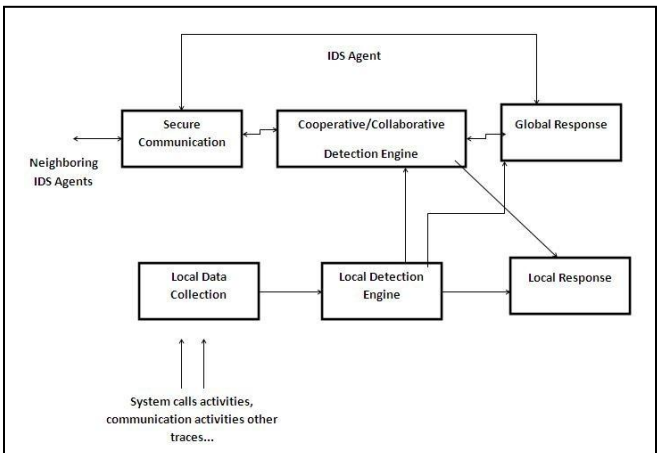

Fig 2: Distributed and Cooperative Intrusion Detection System

ii. Local Intrusion Detection System (LIDS): Albers et al. 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 [3]. Two types of data are exchanged among LIDS: security data (to obtain comple-

mentary information from collaborating nodes) and intrusion alerts (to inform others of locally detected intrusion) [5]. The LIDS architecture is shown in Figure 3, which consists of Communication Framework: To facilitate for both internal and external communication with a LIDS.

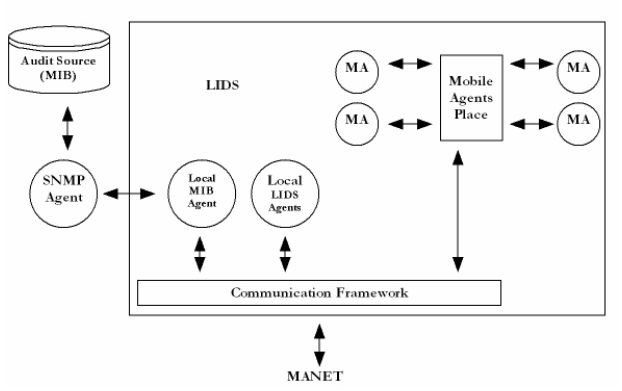

Fig 3: LIDS Architecture in a Mobile Node

iii. Distributed Intrusion Detection System Using Multiple Sensors: Kachirski and Guha proposed a multi-sensor intrusion detection system based on mobile agent technology. The system can be divided into three main modules, each of which represents a mobile agent with certain functionality: monitoring, decision-making or initiating a response. By separating functional tasks into categories and assigning each task to a different agent, the workload is distributed which is suitable for the characteristics of MANETs [10]. In addition, the hierarchical structure of agents is also developed in this intrusion detection system as shown in Figure 4

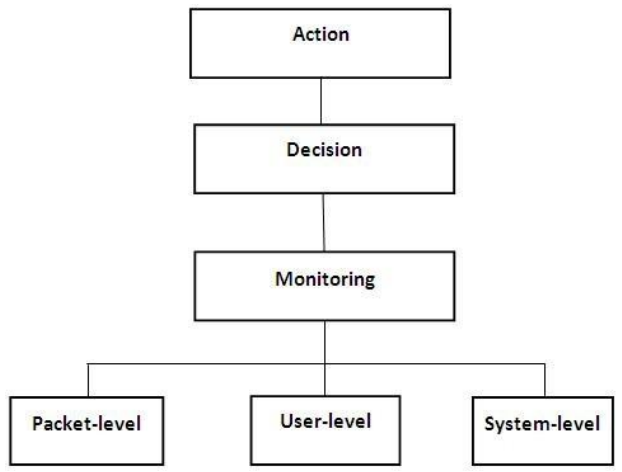

Fig 4: Layered Mobile Agent Architecture

iv. Dynamic Hierarchical Intrusion Detection Architecture: Since nodes move arbitrarily across the network, a static hierarchy is not suitable for such dynamic network topology. Sterne et.al. Proposed a dynamic intrusion detection hierarchy that is potentially scalable to large networks by using clustering and it can be structured in more than two levels as shown in Figure 5. Nodes label1 are the first level cluster heads while nodes labeled 2 are the second level cluster heads and so on [9]. Members of the first level of the clusters are called leaf nodes. Every node has the responsibilities of monitoring, logging, analyzing responding to intrusions detected if there is enough evidence, and alerting or reporting to cluster heads.

7 Issues and Challenges in MANET

A number of restriction and technical difficulties faced by researchers, which are explaining above content.

i. Mobile Ad Hoc Network does not require any infrastructure so it is very difficult to carry out any kind of centralized management and control.
ii. In MANET, IDS monitor the activities and compare the activities against security rules and generate the alarm. Cause of varying topology of network, most IDS tolerates false positive and negative alarm.
iii. To monitor the network activities in coordinated IDS techniques large number of sensors are deployed and finding optimal solution of the sensors requires tactical processing and collecting data from them consume a lot of network bandwidth [3].

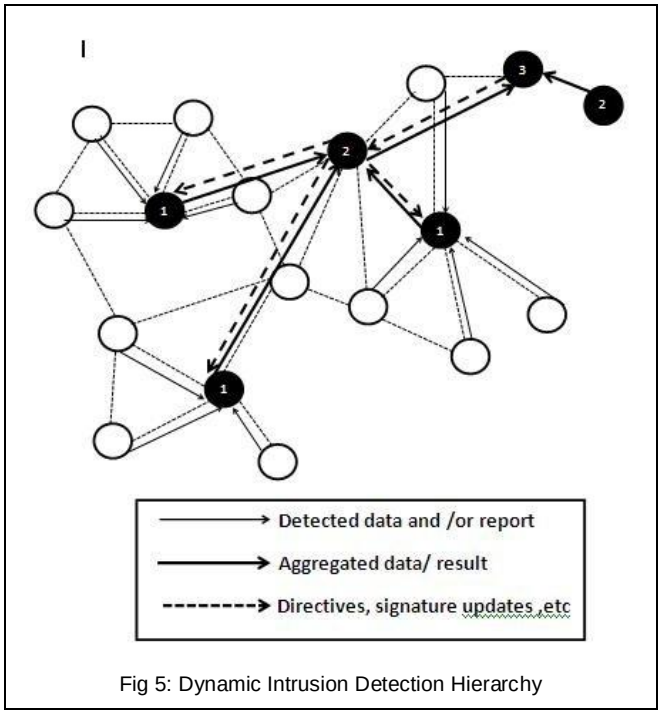

Fig 5: Dynamic Intrusion Detection Hierarchy

8 Conclusion

Intrusion detection and prevention systems are important parts of a well-rounded security infrastructure. IDSs are used in conjunction with other technologies (e.g., firewalls and routers), are part of procedures (e.g., log reviews), and help enforce policies. Each of the IDS technologies—NIDS, WLAN IDS, and HIDS—are used together, correlating data From each

device and making decisions based on what each type of IDS can monitor. Although IDSs should be used as Part of defense in depth (Did), they should not be used alone. Other techniques, procedures, and policies should be used to protect the network. IDSs have made significant improvements in the past decade, but some concerns still Plague our security administrators. These problems will continue to be addressed as IDS technologies improve. As the use of MANET has increased the security in MANET has also become more important accordingly. With the nature of MANET, almost all the intrusion detection system is structured to be distributed and have a cooperative Architecture. Advantage using distributed architecture is the security accident can be detected earlier. However, this Architecture required huge resources, which is difficult to be implemented in small wireless device .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. All attacks exist in wired networks is possible in MANET. MANET has also faces several types of attacks, which are not possible in the traditional wired network, such as selfish attack, black hole attack, sleep deprivation attack and others type of attacks. These attacks occur because of MANET has vulnerable in the use of wireless link, auto-configuration mechanisms, and its routing protocol. Zhang and Sun proposed the IDSs which were designed for detecting the intrusion activities on the routing protocol of MANET. Albers tried to extend the traditional IDS on MANET to detect incoming telnet connections and reacted if they originated from outside community's network. Sterne presented a cooperative and distributed IDS that covered conventional attacks

REFERENCES

[1] John. E. Canavan,"Fundamentals of network security", ISBN 1-56053-176-8

[2] Atul Kahate,"Cryptography and Network security" ISBN 0-07-049483-5

[3] Sanjeev Gangwar,"Mobile Ad Hoc Network: A Comprehensive Study and Survey on Intrusion Detection", http://www.ijera.com/papers/Vol2_issue1/CT21607613.pdf

[4] Jitendra Singh Rathore, "Survey on intrusion detection and prevention system and proposed cost effective solution using software agent". http://ijarcsee.org/index.php/IJARCSEE/article/view/51

[5] Monika Dorji,Bhusan Trivedi,"Survey of Intrusion and Prevention System in MANET basecd on data gathering Techniques", doi: 10.5120/ijais12-450153

[6] Karen Scarfone, Peter Mell. "Guide to Intrusion Detectionand Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology. csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[7] Alberto Grand,"Intrusion Detection and Prevention System" http://www.scribd.com/doc/2096981/Intrusion-Detection-and-Prevention-Systems

[8] Usman Asghar Sandhu , Sajjad Haider , Salman Naseer, Obaid Ullah Ateeb,"A Survey of Intrusion Detection & Prevention Techniques", http://www.ipcsit.com/vol16/13-ICICM2011M035.pdf.

[9] Tiranuch Anantvalee, Jie Wu,"A Survey on Intrusion Detection in Mobile Ad Hoc Networks", http://cis.temple.edu/~jiewu/research/publications/Publication_files/intrusion06.pdf

[10] Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah, "A Survey on MANET Intrusion Detection", http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/Volume2/Issue1/IJCSS-24.pdf

[11] Indraneel Mukhopadhyay, Mohuya Chakraborty,Satyajit Chakrabarti,"A Comparative Study of Related Technologies of Intrusion Detection and Prevention System", www.scirp.org/journal /PaperDownload.aspx?paperID=3823

[12] Paritosh Das, Rajdeep Niyogi, "A Temporal Logic Based Approach to Multi-Agent Intrusion Detection and Prevention", http://interscience.in/IJCNS_Vol1_No1/Paper_10.pdf