Manish Kumar,Dr. M. Hanumanthappa,Dr. T. V. Suresh Kumar/ International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 1, Jan-Feb 2012, pp.274-280

Intrusion Detection Systems Challenges for Wireless Network

Manish Kumar*, Dr. M. Hanumanthappa, Dr. T. V. Suresh Kumar*****

*) Asst. Professor, Dept. of Master of Computer Applications,
M. S. Ramaiah Institute of Technology, Bangalore-560 054, INDIA
**) Dept. of Computer Science and Applications,
Jnana Bharathi Campus, Bangalore University,
Bangalore -560 056, INDIA,
***) Professor & Head, Dept. of Master of Computer Applications,
M. S. Ramaiah Institute of Technology, Bangalore-560 054,

ABSTRACT

Nowadays wireless technology plays an important role in public and personal communication. However, the growth of wireless networking has confused the traditional boundaries between trusted and un-trusted networks. Wireless networks are subject to a variety of threats and attacks at present. An attacker has the ability to listen to all network traffic which becoming a potential intrusion. Intrusion of any kind may lead to a chaotic condition. In addition, improperly configured access points also contribute the risk to wireless network. To overcome this issue, a security solution that includes an intrusion detection and prevention system needs to be implemented. The intrusion detection system is one of the security defense tools for computer networks. In recent years this research has lacked in direction and focus. In this paper we present a survey on the recent progression of multi-agent intrusion detection systems. We survey the existing types, techniques and architectures of Intrusion Detection Systems in the literature. Finally we outline the present research challenges and issues. In addition to examining the challenges of providing intrusion detection in this environment, this paper reviews current efforts to detect attacks against the ad-hoc routing infrastructure, as well as detecting attacks directed against the mobile nodes.

Keywords- **Intrusion Detection System, DIDS, SNORT**

1. Wireless Ad-hoc Networks

The proliferation of mobile computing and communication devices (e.g., cell phones, laptops, handheld digital devices, personal digital assistants, or wearable computers) is driving a revolutionary change in our information society. We are moving from the Personal Computer age (i.e., a one computing device per person) to the Ubiquitous Computing age in which a user utilizes, at the same time, several electronic platforms through which he can access all the required information whenever and wherever needed. The nature of ubiquitous devices makes

wireless networks the easiest solution for their interconnection and, as a consequence, the wireless arena has been experiencing exponential growth in the past decade. Mobile users can use their cellular phone to check e-mail, browse internet; travelers with portable computers can surf the internet from airports, railway stations, Starbucks and other public locations.

Wireless ad-hoc networks do not rely on a preexisting network infrastructure, and are characterized by wireless multi-hop communication. Wireless ad-hoc networks are vulnerable to additional threats above those for a fixed wired network, due to the wireless communication link and the dynamic and cooperative nature of the ad-hoc routing infrastructure. The wireless nature of communication and lack of any security infrastructure raises several security problems.

There are two different types of wireless networks:

- The easiest network topology is where each node is able to reach all the other nodes with a traditional radio relay system with a big range. There is no use of routing protocols with this kind of network because all nodes “can see” the others.

- The second kind uses also the radio relay system but each node has a smaller range, therefore one node has to use neighboring nodes to reach another node that is not within its transmission range. Then, the intermediate nodes are the routers.

The focus is mainly on the security of the routing protocols used in the second kind of ad-hoc network described above.

Any routing protocol must encapsulate an essential set of security mechanisms. These are mechanisms that help prevent, detect, and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are mainly:

- **Confidentiality:** Protection of any information from being exposed to unintended entities. In ad-hoc networks this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed.

- **Availability:** Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g. key management service.

- **Authentication:** Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

- **Integrity**: Message being transmitted is never altered.

- **Non-repudiation***:* Ensures that sending and receiving parties can never deny ever sending or receiving the message.

All the above security mechanisms must be implemented in any ad-hoc networks so as to ensure the security of the transmissions along that network. Thus whenever considering any security issues with respect to a network, we always need to ensure that the above mentioned security goals have been put into effect and none (most) of them are flawed.

Broadly there are two major categories of attacks when considering any network Attacks from external sources and attacks from within the network. The second attack is more severe and detection and correction is difficult. Routing protocol should be able to secure themselves against both of these attacks.

As there is no infrastructure in mobile ad-hoc networks, the nodes have to cooperate in order to communicate. Intentional non-cooperation is mainly caused by two types of nodes: selfish ones that, e.g., want to save power and malicious nodes that are not primarily concerned with power saving but that are interested in attacking the network.

Use of wireless links renders an ad-hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. Eavesdropping might give an attacker access to secret information thus violating confidentiality. Active attacks could range from deleting data, injecting erroneous messages; impersonate a node etc. thus violating availability, integrity, authentication and non-repudiation.

Most of the security measures surrounding ad-hoc networks in general and their routing solutions are, as yet, incomplete and mostly inefficient.

2. Intrusion Detection in Wireless Ad-hoc Networks

Security mechanisms must be deployed in order to counter threats against wireless ad-hoc networks. While cryptographic mechanisms provide protection against some types of attacks from external nodes, cryptography will not protect against malicious inside nodes, which already have the required cryptographic keys. Therefore, intrusion detection mechanisms are necessary to detect these Byzantine nodes. Intrusion Detection Systems (IDS) may be classified based on the data collection mechanism, as well as the technique used to detect events. While the requirement of intrusion detection for both fixed wired and wireless ad-hoc networks are the same, wireless ad-hoc networks impose additional challenges. In general, the effectiveness of solutions designed for fixed wired networks are limited for wireless ad-hoc networks.

2.1. Classifications of IDS

Two distinct types of intrusion detection systems exist. Pattern-based intrusion detection system has the capability to identify all the known intrusions, while anomaly-based intrusion detection mechanisms have the intelligence to identify and respond to new intrusions which are not known. IDS are further classified as Stand-alone IDS, Distributed and Cooperative IDS, and Hierarchical IDS [22]. Stand-alone IDS operates on each node independently to determine intrusions by monitoring the internal events which are recorded in the system logs. In distributed and cooperative IDS, every node participate in intrusion detection and response, while in hierarchical IDS, the cluster-heads monitor all of its child nodes, and respond in case of intrusion is detected.

2.2. Components of IDS

Broadly speaking, IDS has two main components [5], i.e., the features and the modeling algorithm. Features include attributes or measures which are mostly concern with the functionalities the IDS would provide. Algorithm is the core component and the efficiency and accuracy of detecting and responding intrusion is totally dependent on the underlying algorithm. IDS may have many components depend on the nature and characteristics of the network and possible intrusions. Most of the IDS have some common components such as:

- Monitoring Component, this is used for local events monitoring as well as neighbors monitoring.
- Intrusion database, which contains the records of recent misbehaviors and reputation value for the neighbors.
- Response component, which is used to respond in case of intrusion, is detected. The response may be to raise an alarm to alert the administrator or to

broadcast the information to its neighbor nodes about the misbehaving node.

However, the components and the response nature of IDS are mainly dependent on the purpose and services of the IDS. For example, IDS designed for routing misbehavior would have different components and responses as compared to an IDS which is designed for physical and MAC layers anomalies.

3. Wireless Intrusion Detection System

Unlike wired security devices, wireless IDS must monitor the airwaves to detect wireless threats and make active response. Under wireless conditions, IDS should provide particular wireless-specific network threat detection and mitigation against malicious attacks. A common framework for wireless intrusion detection and prevention is shown in Fig 1.

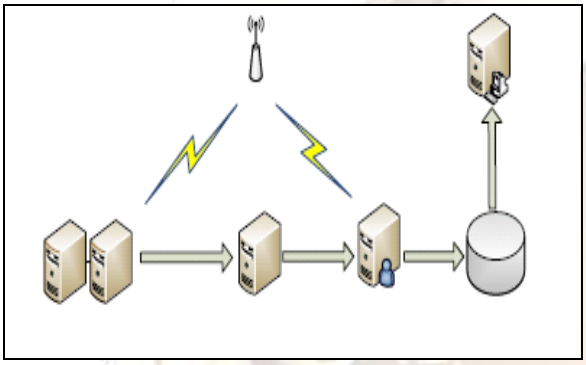

Fig 1:- Wireless Intrusion Detection System Framework

An wireless IDS must have the following basic functions :

- Automatic detection and classification of wireless network threats.
- Accurate plan recognition of continuing attacks by hackers.
- Active response and prevention of the attack behavior that has happened, is happening or will happen.

Although the advantages of IDS are obvious, it needs to consider the system performance since it will increase the network load, resulting in data transmission delay. In order to avoid a system performance bottleneck, IDS must have a wire-speed data processing ability to provide the second layer and third layer of switches, the same processing rate. In improving the accuracy, IDS face greater pressure. Once it makes a wrong decision, it will miss the true attack transactions. IDS solutions for fixed wired networks are often hierarchical and deploy network-based sensors at key traffic concentration points, such as switches, routers, and firewalls. These IDS sensors are physically secured, and use the signature-based detection technique to detect attacks. Alerts generated by these distributed IDS sensors are sent to centralized security servers for analysis and correlation. The centralized security server distributes attack signature updates to the network-based IDS sensors. The effectiveness of IDS solutions that were designed for fixed wired networks are limited for wireless ad-hoc networks as described below:

In the wireless IDS there are still some other drawbacks such as:

A. *Lack of standard wireless architecture:* - In spite of current wireless IDS can prevent some attacks in wireless networks, it cannot provide advanced architecture. It is different from a wired IPS whose location of detectors follows the logical structure of the network, detectors of wireless IDS have to be placed based on physical location. So it makes sense to provide a standard architecture to make the implementation will be more easily.

B. *Less Accurate with high rate of false positives:* - All real time IDS system can suffer from issuing false alarms. Once intrusion is detected, wireless IDS will abandon the data packets, which will form another type of denial of service. This leads to improperly reaction in facing the attack.

C. *Insufficient update of attack signatures:* - An attacker usually at first, need to collect as much as data traffic before attempting an intrusion. This type of passive sniffing is quite dangerous, but there is nothing to do in this direction except to use the proper protection through encryption. In addition, the IDS has a drawback since it only keeps signature files based on known attack pattern recognition files given to them. It only has protection against what are known to be attacks. It does not have sufficient intelligence to recognize all the attacks against the database application, and establishing its update aggressively.

In the wireless IDS there are still some other drawbacks, such as:

- Wireless ad-hoc networks lack key concentration points where network traffic can be monitored. This limits the effectiveness of a network-based IDS sensor, since only the traffic generated within radio transmission range may be monitored.
- In a dynamically changing ad-hoc network, it may be difficult to rely on the existence of a centralized server to perform analysis and correlation.
- The secure distribution of signatures may be difficult, due to the properties of wireless communication and mobile nodes that operate in disconnect mode.
- It may be difficult to physically secure a mobile host that could be captured, compromised, and later rejoin the network as a Byzantine node.

3.1 Related Works

Early IDS design was a host-based architecture, installed as per host basis. Centralized based analysis implemented in many distributed IDS, is prone to several weaknesses as highlighted in [[3] [16] [19]. First, the addition of a new host causes an increment in the load on

the centralize server that performs analysis, raising a scalability issue. Second, communications with the centralized server can overload the network. Third, some of the IDS clients contain platform specific components. These problems have led many researchers to enhance IDS using a multi-agent approach. The features of multi-agent systems (MAS) such as proactive, reactive, social, truthful, benevolent, adaptive, autonomous and rational [8] are the reasons for the adoption of this approach in IDS. MAS support a multi-platform environment. An agent in MAS can be added or removed with minimal impact to the system. Mosqueira-Rey et al. [6] integrated SNORT rules with a detection agent, and compared it with SNORT in term of the rules lookup performance.

Kannadiga and Zulkernine proposed the Distributed Intrusion Detection System using Mobile Agents (DIDM) [19]. One of the components of the DIDMA is the Victim Host List (VHL), used to maintain a list of hosts affected by an attack. An agent is dispatched, moving from one host to another as listed in the VHL. At each visited host, the MA performs aggregation and/or correlation analysis, depending on the type of the attack. It generates summary data and carries it together to the subsequent host. A final decision is made and sent to the IDS Console. In the evaluation, the authors compared the total bandwidth consumed for transmission of collected data from one host to another host by the DIDMA with a centralized based analysis distributed IDS. They found that DIDMA outperforms the other one. DIDMA reduces the network usage as compared to a centralized DIDS. However, there was no security mechanism used to ensure the integrity of data that is carried from one host to another. It was suggested that encryption and authentication are desirable.

Chan and Wei [20] proposed a network based preemptive DIDS. Static agents investigate and obtain evidence data at host basis. Mobile agents move from host to host, collecting evidence data, and preferentially move to a host that has the least load to perform detection analysis. The gateway agent grabs packets from the external network and forwards packets to a suitable controller agent. In most situations, the controller agent at the host manages packets destined to the host. If the host is busy, the controller agent moves to the other host. A cluster of hosts is formed for distributed attacks analysis. The detection agent receives the packet and does the analysis. It will notify the result to a controller agent or if in cluster mode, a leader of controller agents. Then, the result is passed to the policy agent for enforcement. The home agent manages the traffic of packets at the host. The analysis about a particular packet is done just before the arrival of the packet. As the packet arrives, the home agent consults with the policy agent whether to block or to allow the packet. The strength of the approach is that it optimizes the analysis by doing it at the host with least load. The process is migrated to another host if the host is overly loaded with other processes. This system notifies users and blocks the intrusions. However, the solution is prone to the latency effect. Without a proper mechanism, packets grabbed at the gateway may have already arrived and executed before the detection agent makes its decision.

Peddyreddy and Vidal [25] proposed a framework of DIDS with an assumption that agents in the system are isolated from each other and have limited knowledge about any sign of intrusion. Therefore, agents need to negotiate with each other to share some knowledge on a need-to-know basis. The focus is given to a standardized information format and the automation of interaction protocols for effective agent communication. There is an agent at each host, responsible for collecting traces of intrusion, which may come from audit files, log files and processes. The agent analyzes the extent to which the intrusion has compromised the host. The types of information gathered are the type of attack used, the resources accessed, and the subsequent steps performed after obtaining access to the system. This information is passed to other agents so that the intruder's hidden agenda could be detected. When the analysis is done, the agent compares the traces with its stored profiles to look for matching intrusions patterns. It investigates further whether the suspicious activity is explainable with any valid reason. The agent uses a task model in the form of a decision tree to perform various tasks depending on the type of conversation conveyed by other agents. The number of interactions is limited to the agent's need. Finally, the validated intrusion information is displayed to the user.

Ghosh and Sen [1] proposed an Agent-Based Distributed Intrusion Alert System (ABDIAS) that has two primary unique features: the ability to give alerts before an actual attack occurs and the ability to manage compromised hosts based on a distributed decision. The first one is accomplished via information sharing and the beliefs of each agent. The second one is accomplished by the use of a voting method amongagents within a suitable group. The proposed architecture uses knowledge in a Bayesian Network format. In a detection process, if the input is unknown and the value exceeds the threshold, it is considered anomalous. The architecture enables an agent to make an inference about a particular input. Moreover, it can ask other agents for reconfirmation on its inference. Should the result be suspicious, it may ask for a vote from other agents within a group of hosts. If the result is positive, the suspicious agent's host will be isolated from the network. Otherwise, it may ask for a vote from agents in another group.

Mosqueira-Rey *et al.* describe their work in [6] on misused detection (MD) agents as part of their larger work on multi-agent intrusion detection. The MD agent analyzes captured packets and uses known signatures obtained from Snort as a basis for detection. The motivation is to improve the autonomous agent for intrusion detection architecture, introduced by M. Crosbie and G. Spafford's work in [7]. They claim that the autonomous agent has a weakness, as the upper layer in the multi layer agent system may become an attackers' target and if successful, the entire layer can be deactivated. The proposed component uses signatures from

SNORT, supplied into a rule engine called Drools – Jboss. The engine uses the efficient pattern matching called Rete algorithm. Two components of the MD agent are the misuse engine and the packet sniffer. The packet sniffer captures packets and feeds them into the rule engine for detection. The types of possible action that can be taken by the agent are: alert (generate the alert), log (log the packet) and pass (ignore the packet). For the evaluation, the authors compare the performance of both the MD agents against the standard SNORT. Based on their experiment, MD agents perform faster in terms of the number of rules per second and the number of packets per second. The sniffer and detection engine are both pluggable components[11].

3.2 Issues and Challenges

The majority of the past research employed analysis based on data sourced from audit trails, system calls and network traffic. In the network traffic, most research studies looked at the packet header for analysis. Some other research analyzed the payload. Analyzing the packet header is prone to IP address spoofing, while analyzing the payload is prone to data encryption. Several papers also presented the kernel as a data source such as in [12].

Many researchers used KDD CUP 1999 dataset (KDD) in the literature. Mahoney and Chan's 2003 paper [15] harshly criticized the dataset validity. They claimed that the dataset is full of erroneous information and, does not look like a real traffic in many aspects. The claim was supported with an experiment of several IDS using the KDD dataset and their own real network dataset. Based on their meticulous analysis, they conclude that a model with low false alarm, created based on the KDD dataset will tend to generate high false alarm in real environment. Thus, no conclusion or good model can be drawn from the KDD dataset.

There are also efforts to create IDS for applications. The grid computing utilizes a group of machines working together thus the technology requires IDS to provide protection against exploitation and intrusion to the grid itself. In [4], the authors proposed a framework, having a monitoring component that enforces access policy on resources in grid. Correlation and aggregation of active profiles from the computers are compared with the recorded profiles. Yi and Brajendra [10] proposed an IDS for database system using data mining approach. They believed that a legitimate transaction to a particular record must follow a sequence of valid read or write data to related records. Update of record that did not follow the right sequence is subject to intrusive update. However, the solution is only effective for record that has dependency with other records.

The Intrusion Prevention System (IPS) shadows the IDS terminology. Early IDS research studies merely focus on detection. However, later works also suggested the prevention mechanism [9]. Thus, IPS can be described as an extension of IDS. IDS have been associated with anti-virus programs [27] used to prevent unauthorized modification to a specific data store or file structure in a system. They have added diverse features including the addition of the prevention functionality, hardware/software based components and strategic deployment places.

The present patch model provided by many software manufacturers seems a failure, especially when dealing with large scale and fast widespread attacks. The new generation of attacks could cause severe damage to the entire network globally, leaving behind major challenges for future solutions, demanding faster detection of unknown attacks, and able to immunize affected computers.

4. Detection of Attacks Against Mobile Nodes

The requirement for detection of attacks against a mobile node in a wireless ad-hoc network is the same as for hosts in a fixed wired network. In a wired network, hosts are typically protected by network firewalls and network-based IDS [21]. These network-based security mechanisms, however, may not be effective for wireless ad-hoc networks. Without protection from network firewalls, mobile nodes may be directly exposed to attacks from external as well as internal Byzantine nodes. Therefore each mobile node should run some type of node-based IDS, if the node has the available CPU, memory, and battery capacity. While signature-based detection is the primary technique used in fixed wired networks, the secure distribution of signature updates in a wireless ad-hoc network may be difficult, and mobile nodes may operate in disconnect mode. The ideal node based IDS should be able to detect unknown attacks without requiring signature updates. Potential solutions for a node-based IDS to detect attacks against the node may use anomaly or specification-based detection on the system calls generated by monitored processes running on the node. Anomaly detection may be used to detect attacks against a network daemon or a setuserid (SUID) program by building a normal profile of the system calls made during program execution. An intrusion can be detected by comparing the normal profile of a program against a running process. If the process execution deviates significantly from the established profile, an intrusion is assumed. One disadvantage of anomaly detection for mobile computing is that the normal profile must be periodically updated and calculating deviations from the normal profile may impose a heavy load on mobile devices. A more light-weight approach using profiles consisting of the type of system call and it's occurrence of frequency was proposed, in which the DP Matching method (traditionally used in speech recognition) is used to calculate the optimal match between a normal profile and a sample profile [18].

The specification-based technique [13] [14] has demonstrated the capability to detect both known and previously unknown attacks against network daemons and SUID programs on Unix platforms. In this technique, the execution of designated programs is monitored and the generated system calls are compared against a set of predefined constraints. Any deviation from the defined

constraints is considered to be the manifestation of an attack. The specification-based IDS can be preloaded on mobile nodes prior to deployment to the field, and should not require any periodic updates in order to be effective.

5. Architectures for Intrusion Detection in Wireless Ad-hoc Networks

The optimal IDS architecture for a wireless ad-hoc network may depend on the network infrastructure itself. Wireless ad-hoc networks may be configured in either a flat or multi-layered network infrastructure. In a flat network infrastructure, all nodes are considered equal and may participate in routing functions. In a multi-layered network infrastructure, all nodes are not considered equal. Nodes within transmission range are organized into a cluster, and elect a Cluster-Head (CH) node to centralize routing information for the cluster. The CH nodes form a virtual backbone for the network, and depending on the protocol intermediate gateway nodes may relay packets between CH nodes. This infrastructure be suitable for military applications.

5.1 Stand-alone IDS Architecture

In a stand-alone IDS architecture, each host runs an IDS that independently detects attacks. The original IDS were stand-alone systems developed to protect specific mainframes. Since stand-alone IDS do not cooperate or share information with other systems, all intrusion detection decision are based on information available to the individual node. The watchdog mechanism [17][26], could be deployed as a stand-alone IDS mechanism and detect Byzantine nodes within transmission range, but not report these malicious nodes to any other node. The node running watchdog would then forward packets only to neighboring nodes that do not appear to misbehave. While the effectiveness of this solution is limited, this architecture may be suitable in an environment where not all nodes are capable of running an IDS or have an IDS installed.

5.2 Distributed and Cooperative IDS Architecture

Intrusion detection for fixed wired network is primarily hierarchical and network-based, so there is no need to incur the overhead associated with the exchange of messages required for this architecture. This IDS architecture is more suitable for flat wireless ad-hoc networks, and a distributed and cooperative architecture was proposed for this environment in which IDS agents residing on every node independently make local intrusion detection decisions, but cooperatively participate in global intrusion detection [14]. In this architecture, if a node detects an intrusion with weak or inconclusive evidence, it can initiate a cooperative global intrusion detection procedure, or if a node detects locally an intrusion with strong evidence, it can independently determine an attack on the network. A cooperative and distributive IDS architecture could be susceptible to attacks from Byzantine nodes, which could independently make false claims of detecting an attack from a correct node with strong evidence, thus making it difficult to derive a distributed consensus.

5.3 Hierarchical IDS Architecture

Hierarchical IDS architectures have been proposed for multi-layered, wireless ad-hoc networks. In a multilayered wireless ad-hoc network, cluster-head nodes centralized routing for the cluster and may support additional security mechanisms. A Byzantine CH nodes could potentially reroute, modify, or drop packets transmitted by cluster member nodes, as well as any packets routed through the CH node on the virtual backbone

6. Intrusion Response in Wireless Ad-hoc Networks

The ideal intrusion response for a wireless ad-hoc network is to isolate Byzantine nodes from the rest of the network. For fixed wired networks, the "electronic quarantine" was developed to dynamically create the filtering rules required for desktop firewalls, packet filtering intranet firewalls, and application-level Internet firewalls, in order to isolate a compromised host within a fixed wired network [2]. In a dynamically changing wireless ad-hoc topology, the centralized solution proposed by the electronic quarantine would not be effective, since the implementation of intranet firewalls and application-level firewalls may not be feasible. In the distributed and cooperative IDS architecture proposed for wireless ad-hoc networks, one approach suggested that in response to a detected intrusion end users re-authenticate themselves using an out-of-bound mechanism, and negotiate a new communication channel to exclude compromised nodes [28]. Re-authentication using an out-of-bound mechanism may be appropriate in some but not all environments.

7. Conclusion

The intrusion detection system has been an active research area for more than half a century. The widespread use of the Internet increases the number of intrusion incidents from year to year making the research area remain relevant.

In this paper, we surveyed trends in multiagent IDS research. The benefits of multiagent are mentioned in section four. However whether multiagent in IDS outperforms its counterpart is debatable since the detection ability is in fact determined by the technique and algorithm. We have outlined a number of research issues in the subject area. Our future work includes a development of a novel architecture for an effective defense against malicious code attack, inspired by the human immune system. We introduce two phases of program execution. The first phase uses a malware profile pattern matching mechanism, whereas the second phase uses a program profile matching mechanism. In the first phase, if a running executable is detected as containing malicious code, it is quarantined and its file signature is subsequently used to scan the same file at certain intervals. In the second phase, a deviation against its own profile reverts the executable to the first phase.

References

1 A. Ghosh and S. Sen, "Agent-Based Distributed Intrusion Alert System," in Distributed Computing, 2004, pp. 240-251.

2 Brutch, P., Brutch, T., and Pooch, U. "Electronic Quarantine: An Automated Intruder Response Tool", In *Proceedings of Information Survivability Workshop*, 1998.

3 Buchegger, S. and Boudec, J. "Performance Analysis of the CONFIDANT Protocol Cooperation of Nodes: Fairness in Dynamic Ad-ho Networks)", In *Proceedings of MOBIHOC '02*, 2002.

4 C. Ong Tian and A. Samsudin, "Grid-based intrusion detection system," in The 9th Asia-Pacific Conference on Communications, 2003, pp. 1028-1032 Vol.3.

5 Djenouri D., Khelladi L., and Badache N., "A Survey of Security Issues in Mobile Ad-hoc and Sensor Networks," *Computer Journal of IEEE Communications Surveys and Tutorials*, vol. 7, no. 4, pp. 1-15, 2005.

6 E. Mosqueira-Rey, A. Alonso-Betanzos, B. del Río, and J. Piñeiro, "A Misuse Detection Agent for Intrusion Detection in a Multi-agent Architecture," in Agent and Multi-Agent Systems: Technologies and Applications, 2007, pp. 466-475.

7 E. H. Spafford and D. Zamboni, "Intrusion detection using autonomous agents," Computer Networks, vol. 34, pp. 547-570, 2000.

8 F. Bellifemine, G. Caire, and D. Greenwood, Developing Multi-Agent Systems with JADE: Wiley, 2007.

9 F. Gong, "Next Generation Intrusion Detection Systems (IDS)," McAfee Inc, November 2003, p. 14.

10 H. Yi and P. Brajendra, "A data mining approach for database intrusion detection," in Proceedings of the 2004 ACM symposium on Applied computing Nicosia, Cyprus: ACM, 2004.

11 J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isacoff, E. Spafford, and D. Zamboni, "An architecture for intrusion detection using autonomous agents," in Proceedings of the 14th Annual Computer Security Applications Conference, 1998, pp. 13-24.

12 K. Byung-joo and K. Il-kon, "Kernel based intrusion detection system," in Fourth Annual ACIS International Conference on Computer and Information Science, 2005, pp. 13-18.

13 Ko, C., Ruschitzka, M., and Levitt, K. "Execution Monitoring of Security Critical Programs in Distributed Systems: A specification-based approach," In *Proceedings of Symposium on Security and Privacy*, 1997.

14 Ko, C., Brutch, P., Rowe, J., Tasfnat, G. and Levitt, K., "System Health and Intrusion Monitoring using a Hierarchy of Constraints", In *Proceedings of 4th International Symposium on Recent Advances in Intrusion Detection*, 2001.

15 M. V. Mahoney and P. K. Chan, "An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection," in Recent Advances in Intrusion Detection, 2003, pp. 220-237.

16 Mohd Fadzli Marhusin, David Cornforth, Henry Larkin, "An Overview of Recent Advances in Intrusion Detection"School of ITEE, The University of New South Wales at Australian Defence Force Academy, Canberra 2600 ACT, Australia

17 Marti, S., Giuli, T., Lai, K., and Baker, M., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," In *Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking*, 2000.

18 Okazaki, Y., Sato, I., and Goto, S., "A New Intrusion Detection Method based on Process Profiling", In *Proceedings of 2002 Symposium on Applications and the Internet (SAINT '02)*, 2002.

19 P. Kannadiga and M. Zulkernine, "DIDMA: a distributed intrusion detection system using mobile agents," in Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks 2005, pp. 238-245.

20 P. C. Chan and V. K. Wei, "Preemptive distributed intrusion detection using mobile agents," in Proceedings of Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2002), 2002, pp. 103-108.

21 Paul Brutch, Calvin Ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks" Network Associates Laboratories

22 Siddiqui S. and Hong S., "Security Issues in Wireless Mesh Networks," *in Proceedings of IEEE International Conference on Multimedia and Ubiquitous Engineering*, Korea, pp. 178-182, 2007.

23 Shafiullah Khan,Kok-Keong Loo, and Zia Ud Din, " Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks "

24 S. B. Jeong, Y. W. Choi, and S. Kim, "An Effective Placement of Detection Systems for Distributed Attack Detection in Large Scale Networks," in Information Security Applications, 2005, pp. 204-210.

25 T. D. Peddireddy and J. M. Vidal, "Multiagent network security system using FIPA-OS," in Proceedings of IEEE SoutheastCon, 2002, pp. 229-233.

26 White, G. and Pooch, U., "Cooperating Security Managers: Distributed Intrusion Detection System," *Computers & Security*, vol. 15, no. 5, 1996.

27 X. Kun, Z. Ji, W. Xin, and X. Xiangyang, "A Novel Peer-to-Peer Intrusion Detection System," in Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies 2005, pp. 441-445.

28 Zhang, Y. and Lee, W., "Intrusion Detection in Wireless Ad-Hoc Networks," In *Proceedings of the Sixth Annual International Conference on Mobile Communication and Networking*, 2000.