Computer and Information Science; Vol. 5, No. 4; 2012
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

A Comprehensive Survey on Anomaly-Based Intrusion Detection in MANET

Davood Kheyri[1] & Mojtaba Karami[1]

[1] Department of Electrical and Computer Engineering, Islamic Azad University Hamedan Branch, Hamedan, Iran

Correspondence: Mojtaba Karami, Department of Electrical and Computer Engineering, Islamic Azad University Hamedan Branch, Hamedan, Iran. E-mail: karami@iauh.ac.ir

Received: September 21, 2011 Accepted: October 1, 2011 Online Published: June 25, 2012

doi:10.5539/cis.v5n4p132 URL: http://dx.doi.org/10.5539/cis.v5n4p132

Abstract

In recent years, mobile ad hoc networks (MANET) have become an interesting research area. This type of networks have a salient characteristics compare with wired networks which are more vulnerable. Nowadays, for the network security, defend in depth strategies are used. One of them is intrusion detection system (IDS). Many intrusion detection techniques developed for weird networks however, because the nature of MANET we cannot apply them directly in MANET. According to detection techniques, IDSs can be classified into three categories as follows: Misuse-based detection, Anomaly-based detection, and Specification-based detection.

In this paper, we are going to evaluate anomaly-based intrusion detection techniques proposed for MANET. For this, we present a comprehensive survey about anomaly based intrusion detection techniques. Afterward we evaluate their performance, advantages, and disadvantages. As a result constantly, we will understand MANET's security problems based on which we can suggest solutions for future research.

Keywords: mobile ad hoc networks (MANETS), intrusion detection systems, anomaly detection, security

1. Introduction

A mobile ad hoc network is a collection of mobile nodes that communicate with each other via wireless links, directly or relying on other nodes as routers. Their main advantage is flexibility, adaptability, easily cooperation and efficient communication in environments without the help of any fixed infrastructure or centralized management point.

Despite many advantages, these type of networks are inherently vulnerable to various attacks due to some features such as open medium, dynamic topology, lack of centralized management and control points and etc (Huang & Wenke, 2003). Therefore, today's concepts of defend in depth for security in networks are used. The First layer is prevention layer (e.g. Firewall, authority, and coding) and the second one is intrusion detection system that is used to detect intruder attack to networks and to produce suitable response. Nowadays, also the technology for manufacturing wireless instruments develops, the capabilities of these instruments (like battery, CPU power, memory capacity) increase, too. However, new attacks against the MANET are increase continuously. So the intrusion detection system should be able to detect these new and unknown attacks. The anomaly-based IDS is one of the techniques that has the ability to detect the unknown attacks. In recent years, many IDSs based on the three detection techniques were presented for the MANET. Since most of the work was done based on the anomaly-based technique, in this article we investigate the work done in the anomaly-based domain and represent their strong and weak points.

The structure of this article is as follow: In section 2, Classification and architectures for intrusion detection systems are presented; In section 3, anomaly-based detection techniques are analyzed; In section 4, anomaly-based detection systems proposed will be evaluated; In section 5, we'll discuss categorization of IDS's and finally in section 6, we will arrive at conclusions and will propose some suggestions for future research.

2. Intrusion Detection Systems

Because of the nature of the MANETs, their security is a vital issue. So, nowadays, to secure these networks, a multi-layer protection is used. The intrusion detection system, as the second protection layer, is a process that controls the behaviors and activities in order to detect the illegal and abnormal activities.

2.1 Classification of Intrusion Detection System

As shown in Figure 1, According to data collection mechanisms, IDSs can be classified into two categories as follows (Stamouli, 2003): Host-based and Network-based. *Network-based IDS* runs on a gateway of a network and obtained audit data from traffic that flows through it, And then are analyzed the data collected. While *Host-based IDS* acquires this data through hope rating system's log files that runs on the node. Also according detection technique, IDSs can be classified into three categories as follows (Mandala et al., 2008; Hijazi & Nasser, 2005): misuse-based (or signature-based) detection, anomaly-based detection, and specification-based detection.

In *signature-based* method, known patterns of attacks are kept. Then the behavior of the network and its nodes is controlled and when any suspicious behavior is observed, it is compared with the existence patterns to detect the intrusion. If a behavior matches with existence patterns, it is considered as an attack. In *anomaly-based* technique, normal behavior of the target system (network and nodes) is defined, and then a profile or normal behavior model is constructed according to it. Then based on this profile a threshold is defined, which shows the boundary of normal and abnormal behaviors. Then the nodes and the network are controlled and if any behavior unmatched with the normal behavior is observed, it is considered as an attack. In the *specification-based* technique, system defines a set of constraints that describe the correct operation of a programs or protocol. Then it monitors the execution of the program or protocol whit respect to the defined constraints. If a behavior is deviated with these constraints, it is reported as an attack (Ko et al., 2001).

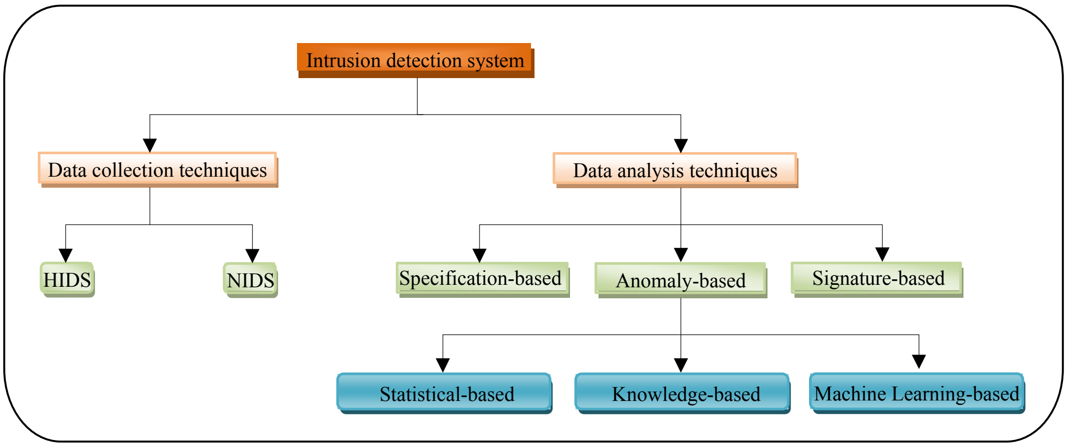

Figure 1. Classification of intrusion detection system

2.2 Architecture of IDS

According to the infrastructure of the network, MANETs can be framed in two ways: flat or multi-layer ones. This framing depends on the expected function. So a suitable and efficient IDS architecture depends highly on the infrastructure of the network itself. There are four major architectures for the MANETs as follow (Menaria et al., 2010):

2.2.1 Stand-alone Intrusion Detection Systems

In this architecture, An IDS is implemented on each node and does the operation of intrusion detection. Whatever decision is made by each node is based on the information of the node itself, and there is no cooperation among the nodes of the network. In stand-alone architecture, because there is no cooperation and interchange on information among the IDS and also the extent of view of each node on the network is limited, the intrusion detection operation has a low accuracy. Because of this reason, this kind of architecture is rarely applied in MANET.

2.2.2 Distributed and Cooperative Intrusion Detection Systems

In this architecture, each node participates in the intrusion detection operation and responding to it, by executing an IDS agent on itself. An agent is responsible for detection and collection of the incidents and local information in order to detect the possible intrusions and to produce a suitable response independently. In case that the node doesn't have enough information and documents for detection of the intrusion, it cooperates with the agents of the neighboring IDS and commits the intrusion detection operation thoroughly.

2.2.3 Hierarchical Intrusion Detection Systems

This developed architecture is a distributed and cooperative one. In this architecture, the nodes take different tasks based on their level in the hierarchy. As an example, in comparison to other ordinary nodes in the cluster, the cluster-head has a range of extra responsibilities like sending routing packets to the whole cluster. The cluster-heads of the MANET act as strategic points (like gateways or switches in wired networks). In this architecture, the cluster-heads are responsible for detecting the intrusion and creating a suitable response throughout the cluster level.

2.2.4 Mobile Agent for Intrusion Detection Systems

Mobile agents are applied in MANETs as a concept in the same intrusion detection techniques. These agents can move easily throughout a major network and each has a specific duty. Because one or more agents can be placed inside a node, the intrusion detection operation can be distributed throughout the network. There are several privileges in using the mobile agents. For example, some operations are not proportioned to every node. And because of this, there will be a decrease in consuming the resources. The mobile agents-based IDS can be considered as a kind of distributed and cooperative IDS. Some techniques also use the combination of the mobile agents with hierarchical IDSs.

3. Anomaly-Based Detection Techniques

Anomaly-based detection techniques can be classified in to three groups according to the processing type of behavior model of the target system: statistical-based, knowledge-based and machine learning-based (Lazarevic, 2005).

3.1 Statistical-Based Techniques

In statistical-based techniques, the traffic activities of the network are monitored and profile is created that shows network normal behavior. This profile constructed based on some metrics, such as traffic rate, number of the packets for each protocol, communication rate and different IP addresses. During the process of detection, two groups of data on network traffic are considered. A set is related to the currently observed profile and the other is related to the normal profile. When an anomaly occurs in the network, the current profile is created and an anomaly privilege is calculated by comparing the current and normal profile. This privilege shows the degree of abnormality for a given anomaly. When the privilege exceeds the defined threshold, the intrusion detection system reports the incidence of an anomaly. The advantages of the statistical-based method are: firstly it doesn't require the background knowledge about the target system's normal activity. In this technique, system can obtain behaviors and activities of nodes by monitoring them, Secondly statistical methods provide exact reports on malicious activities which are done during a long period. Yet, this method has its own disadvantages: firstly it is susceptible to mistake by attacks, in the way that the traffic created during attacks in the network may be considered as normal activities, secondly settings related to the amount of different parameters, specially creating an efficient balance between false positive and false negative is difficult in reality (Denning & Neumann, 1985; Ye et al., 2002).

3.2 Knowledge-Based Techniques

Knowledge-based techniques are widely used in expert systems (Lunt et al., 1988). These systems are for classifying the audit data and are based on a set of specific rules. It contains three stages: first according to the data gathered during the process of training, different features and classes are resulted. Then in the second stage a set of necessary rules are extracted to classify the parameters or functions. Finally, in the third stage, the gathered data are classified according to these rules. This model can be created manually by a human expert through a set of rules, which are applied to determine the legal behaviors of the system. If the specifications are complete enough, this model will be able to detect illegal behavior patterns, then as a result, the false positive rate will decrease. Specifications could also be developed by using some kind of formal tools. For example, the finite state machine (FSM) approach, a sequence of states and transitions among them is created for modeling network protocols behaviors. The most significant advantages of current approaches to anomaly detection are those of robustness and flexibility. Disadvantage is that the development of high-quality knowledge is often difficult and time-consuming (Anderson et al., 1995; Estévez-Tapiador et al., 2003; Sekar et al., 2002).

3.3 Machine Learning-Based Techniques

Machine learning techniques are based on either an explicit or implicit model. These techniques based on created model can categorize pattern of observed behaviors. The main characteristic of these techniques is needed to labeled data in order to learn the behavior model of the nodes and the whole network. This operation severely requires the resources such as energy and bandwidth. The causes contain the action of labeling the data and the detection and separation this labeled data among the huge amount of the data demands high resource.

In many cases, the function of principle of machine learning is simultaneous with statistical techniques. In these cases, the constructor of the model in addition to use of the statistical techniques uses the results of the previous stages to improve the performance of intrusion detection system. So a machine learning-based anomaly detection is able to change its strategy to obtain the new information. Although this features can make it desirable to use these techniques for all conditions. Nevertheless, the key problem related to these methods is costly nature of them in terms of required resources. Several machine learning-based schemes have been used in anomaly-based detection technique such as: Bayesian network (Kruegel et al., 2003), Markov models (Yeung & Ding, 2003; Estévez-Tapiador et al., 2005; Mahoney & Chan, 2002), neural network (Ramadas et al., 2003; Cansian et al., 1997), fuzzy logic technique (Dickerson, 2000; Bridges & Vaughn, 2000), genetic algorithms (Li, 2004) and clustering detection (Liao & Vemuri, 2002).

4. Analysis and Evaluation of Anomaly-Based Detection System

In this section, we present the newest anomaly-based detection systems, which are proposed for MANET, and we will mention their main capabilities, advantages and disadvantages.

Lee, Zhang and Huang (Zhang et al., 2003; Zhang & Lee, 2000) proposed an anomaly-based detection system that is cooperative and distributed. In this system, each node independently detects local intrusions and gathers information by using an IDS agent. And if needed, it cooperates with other neighboring IDS agents to increase the accuracy of detection. In this system, each operation is done by a given module in the agent. The key advantage of the system is that it is distributive and cooperative, and consequently it increases the accuracy. Its main disadvantage is that the responding time and the rate of false positive are high.

Kachirski and Guha (2003) proposed a multi sensor anomaly-based detection system that is based on the mobile agent technology. This system uses three main agent, monitoring, decision and action to detect the intrusion. The monitoring agent supervises the network and the nodes, the action agent is responsible for producing suitable response against the intrusion and the decision agent analyzes the gathered data for detection of intrusion. This system is based on hierarchical structure and the agents. These agents are placed on nodes based on their function. Therefore, the action agent is placed on all nodes of the network and the decision agent is placed on some of nodes.

The most important advantage of the system is applying the distributed mobile agents. Moreover, its most important disadvantage is that finding suitable nodes to appoint to main tasks is time-consuming and is more complex.

Sun et al. (2003) introduces a zone-based anomaly detection system. In this system, MANET is divided to several non-overlapping zones. In this system, the nodes are organized in two layers, intra-zone and inter-zone (or gateway nodes). Each node has an IDS agent that is executed on it. Other components of this system are data collection module, detection engine, local aggregation and correlation engine (LACE) and global aggregation and correlation engine (GACE). The data collection module and the detection engine are responsible for gathering the audit data and analyzing every instant of intrusion respectively. The LACE module is responsible for correlation and aggregation of the local reported alerts. These alerts are broadcast for all nodes in the same zone. The function of GACE in this system is depends on the type of the node. If node is an intra-zone one, it just sends the reports to the inter-zone nodes. And if the node is an inter-zone one, it receives the reports from other intra-zone nodes, aggregates and correlates them and compares with its own reports and if needed it creates some alerts. The intrusion response module is responsible to produce suitable respond against the detected intrusion. In addition, this module is responsible to managing alerts received from GACE. The key advantage of the system is dividing the network into non-overlapping zones and its main disadvantage is that the responding time is long.

Nakayama et al. (2009) proposed an anomaly-based detection system to detect malicious activities that target at the AODV routing protocol (Perkins et al., 2011). The proposed system uses the machine learning technique to detect the intrusion. So, after gathering the data step, then an approximate distribution of the normal behavior is extracted. Then by analyzing the gathered data and compare it with approximate distribution, system can find any deviation from normal behavior. If the deviation exceeds the threshold, the system realizes that an attack was occurred. The main advantage of this system is the low rate of the false positive and the key disadvantage is that it cannot be used for detection of all possible attacks.

Joseph et al. (2011) proposed an anomaly-based detection system in the MANET to detect sinkhole attack (like those nodes that do not cooperate with the network in routing and forwarding operation). This system by a classifier can detect malicious behaviors. This system can gathered data from the network, MAC and physical layers. Then by processing the gathered data by the classifier, a function created to make the decision. This function will distinguish whether the current event is legal or it is a result of sinkhole attack. The main advantage of this system is using the features of several layers and its main disadvantage is that it is used just to detect one type of sinkhole attack.

Lauf et al. (2010) proposed a two-stage anomaly-based detection system. Its goal is to act in environments with limited resources, like the MANETs. This detection system can be divided into two stages. The first stage for fast detection of the threat and, then compute a threshold for the second stage. While the second stage aims at exactly detecting the resources of the threat and also for detecting repeated attacks simultaneously. At the first stage in this system, an analysis is done on the gathered data, if any deviation was detected, then second stage is called. The main advantage of this system is that needed minimum amount of the resource. Because it is called the second stage only if it needed. The main disadvantage of the system is the high rate of the false positive.

Kabiri and Aghaeiin (2011) present an anomaly-based technique that focuses on denial of service (dos) attacks. The proposed system gets benefit from its neighbors' normal behaviors and analysis them based on the optimal features. Its main advantage is that it reduce the computational and data processing overhead by using a set of the optimal features. The key disadvantage of the system is that the system is exposed to high rate of false positive.

Nadeem and Howarth (2009) proposed an anomaly-based detection system for MANET to detect dos attacks. The proposed system detects the malicious behaviors based on statistical analyses. In this system, after gathering data, its probability distribution is estimated and it is compared with normal behavior by using chi-square test (Lancaster, 1969). If the distribution of the gathered data does not fit the normal behavior, then the observed behavior is considered as a suspicious. For every suspicious behavior, the counter increased a unit. Besides, in the case of exceeding the threshold, the node will be labeled as malicious. The main advantage of this system is the low rate of false positive and its main disadvantage is that it is just able to detect dos attacks.

5. Discussion and Summary

Nowadays, the use of mobile networks, especially the MANET is increasing. Therefore, it is very important to pay attention to their problems and deficiencies especially those related to the security. One way to secure them is by utilizing intrusion detection systems (IDSs). Many IDSs have been proposed for this type of networks. Because of the nature of the MANET, many of these IDSs have distributed and cooperative architecture and in generally they using the concept of the mobile agent (Zhang et al., 2003; Zhang & Lee, 2000; Kachirski & Guha, 2003; Sun et al., 2003; Joseph et al., 2011; Nadeem & Howarth, 2009). One of the advantages of this architecture is exactly detecting the attacks and their resource; also produce global responding to these attacks. However, the main disadvantage of this architecture is that it imposes communication and processing overload, and consequently the need to great amount of resources (especially energy and the bandwidth) is increases. So nowadays, in order to decrease the consumption of the resources, and parallel acts of the nodes in the process of detecting the intrusion, a hierarchical structure is used (Kachirski & Guha, 2003; Sun et al., 2003). The nodes are placed in several levels according to their positions and status in this structure. Then each node gets responsibilities suitable with its level. The main problem of this architecture is the problem called single of failure. It means that, the high-level nodes that have key responsibilities when compromised or be misbehavior, whole network will be broken. Since some of attacks occur only in a single layer or specific layers, and also one layer may be gives comprehensive information to IDS than other layers (like the dos attack that can be occur in the several layers, the application layer can gives more exact information in comparison with lower layers). So nowadays, many of the proposed IDSs have cross-layer architecture (Joseph et al., 2011). Table 1 summarizes the structure, advantage and disadvantages of each of the mentioned architectures in this article.

6. Conclusion and Further Guidelines

As Table 1 shows, much of the works done in the IDS's area in the MANET are based on anomaly techniques. Therefore, it is necessary to use new and suitable techniques and methods to construct the nodes' and networks' normal profile, and also to define the threshold. One of these new techniques that can be applied in future researches is the use of the game theory and the Bayesian networks. Since it is excepted that novel attacks will be launched against the MANET, it is necessary more pay attention to anomaly-based techniques than other ones. Also is better the using of combined techniques (such as anomaly-based technique alongside one of the signature-based or specification-based techniques). Another hot area for further research is preventing and detecting those attacks that aimed at IDS itself. Because the previous works were focused on protecting the mobile nodes and data against the attacks.

Table 1. Comparison of anomaly-based intrusion detection systems

Author(S)	Zhang et al., 2003	Kachirski & Guha, 2003	Sun et al., 2003	Nakayama et al., 2009	Joseph et al., 2011	Lauf et al., 2010	Kabiri et al., 2011	Nadeem & Howarth, 2009
Detection Engine Technique	using two engine technique: local and global detection engines	Using statistical techniques with mobile agents	using zone-based detection with markov chain	Using machine learning to create a dynamic profile	using a classifier for classified gathered data from cross-layer	using two engine technique: engine for setting threshold and engine for detection the main causes of the attacks	Monitor and create a dynamic profile for neighbors	create a dynamic profile using statistical techniques with chi-square test
Detection Technique	anomaly	anomaly	anomaly	anomaly	anomaly	anomaly	anomaly	anomaly
Routing Protocol	AODV, DSR DSDV	undefined	DSR	AODV	OLSR	undefined	DSR AODV	AODV
Addressed Attacks Type	routing errors, packets dropping	undefined	routing attacks, destruction attacks	routing attacks, packets dropping	sinkhole	spoofing and mislead attacks	DOS	DOS
Number of Nodes	undefined	10-100	30	50-100	30-50	35	20-50	25-64
Environment	simulation	simulation	simulation	simulation	simulation	simulation	simulation	simulation
Advantages	High accuracy, adaptability to topology changes, using the cross-layers technique	the use of distributed mobile agents, incurs light computational overhead	network is divided into non-overlap zones, reduce process of intrusion detection overhead by using zone-base detection	adaptability to network changes	cross - layer monitoring	increased detection accuracy, scalability, incurs less processing overhead	uses an optimal set of features, incurs less processing overhead	adaptability to network changes
Disadvantages	High response time and rate of false positive	Expensive and time consuming to selecting nodes for key task assignment	high response time, it used only for the dsr protocol	false negative become part of the normal profile, incurs extra processing overhead, cannot detect all possible attacks	can only detect sinking attacks	high ratio of false positive, define a suitable threshold is very complex	high ratio of false positive, can only detect dos attacks	false negative become part of the normal profile, incurs extra processing overhead, can only detect dos attacks
Disadvantages	High response time and rate of false positive	Expensive and time consuming to selecting nodes for key task assignment	high response time, it used only for the dsr protocol	false negative become part of the normal profile, incurs extra processing overhead, cannot detect all possible attacks	can only detect sinking attacks	high ratio of false positive, define a suitable threshold is very complex	high ratio of false positive, can only detect dos attacks	false negative become part of the normal profile, incurs extra processing overhead, can only detect dos attacks

References

Anderson, D., Lunt, T. F., Javitz, H., Tamaru, A., & Valdes, A. (1995). *Detecting unusual program behavior using the statistical component of the next-generation intrusion detection expert system (NIDES).* Menlo Park, CA, USA: Computer Science Laboratory, SRI International, SRIO-CSL-95-06.

Bridges, S. M., & Vaughn, R. B. (2000). Fuzzy data mining and genetic algorithms applied to intrusion detection. *Proceedings of the National Information Systems Security onference,* 13-31.

Cansian, A. M., Moreira, E., Carvalho, A., & Bonifacio, J. M. (1997). Network intrusion detection using neural networks. *International Conference on Computational Intelligence and Multimedia Applications (ICCMA'97),* 276-280.

Denning, D. E., & Neumann, P. G. (1985). *Requirements and model for IDES - a real-time intrusion detection system*. Computer Science Laboratory, SRI International.

Dickerson, J. E. (2000). *Fuzzy network profiling for intrusion detection.* Proceedings of the 19th International Conference of the North American Fuzzy Information Processing Society (NAFIPS).

Estévez-Tapiador, J. M., García-Teodoro, P., & Díaz-Verdejo, J. E. (2003). *Stochastic protocol modeling for anomaly based network intrusion detection* (pp. 3-12). Proceedings of IWIA, IEEE Press.

Estévez-Tapiador, J. M., García-Teodoro, P., & Díaz-Verdejo, J. E. (2005). *Detection of web-based attacks through Markovian protocol parsing* (pp. 57-62). Proc. ISCC05.

Hijazi, A., & Nasser, N. (2005). *Using Mobile Agents for Intrusion Detection in Wireless Ad Hoc Networks.* Wireless and Optical Communications Networks (WOCN).

Joseph, J. F. C., Lee, B. S., Das, A., & Seet, B. C. (2011). Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA. *Dependable and Secure Computing, IEEE Transactions, 8*(2), 233-245.

Kabiri, P., & Aghaei, M. (2011). Feature Analysis for Intrusion Detection in Mobile Ad Hoc Networks. *International Journal of Network Security, 12*(2), 80-87.

Kachirski, O., & Guha, R. (2003). *Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks*. Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03), IEEE.

Ko, C., Rowe, J., Brutch, P., & Levitt, K. (2001). *System Health and Intrusion Monitoring Using a hierarchy of Constraints.* Proceedings of 4th International Symposium, RAID.

Kruegel, C., Mutz, D., Robertson, W., & Valeur, F. (2003). *Bayesian event classification for intrusion detection*. Proceedings of the 19th Annual Computer Security Applications Conference. http://dx.doi.org/10.1109/CSAC.2003.1254306

Lancaster, H. O. (1969). *The Chi-Squared Distribution.* Wiley Publications in Statistics.

Lauf, A., Peters, R. A., & Robinson, W. H. (2010). A Distributed Intrusion Detection System for Resource-Constrained Devices in Ad Hoc Networks. *Journal of Ad Hoc Networks, 8*(3), 253-266.

Lazarevic, A., Kumar, V., & Srivastava, J. (2005). *Intrusion detection: a survey, Managing cyber threats: issues, approaches, and challenges* (pp. 330).Springer Verlag.

Li, W. (2004). *Using genetic algorithm for network intrusion detection* (pp. 1-8). C.S.G. Department of Energy.

Liao, Y., & Vemuri, V. R. (2002). Use of K-nearest neighbor classifier for intrusion detection. *Computers & Security, 21*(5), 439-448. http://dx.doi.org/10.1016/S0167-4048(02)00514-X

Lunt, T. F., Jagannathan, R., Lee, R., Listgarten, S., Edwards, D. L., Neumann, P. G., …Valdes, A. (1988). *IDES: The Enhanced Prototype C a Realtime Intrusion- Detection Expert System.* Technical Report SRI-CSL-88-12, SRI International, Menlo Park, CA.

Mahoney, M. V., & Chan, P. K. (2002). *Learning nonstationary models of normal network traffic for detecting novel attacks*. Proceedings of the Eighth ACM SIGKDD, pp. 376-385.

Mandala, Ngadi, M. A., & Abdullah, A. H. (2008). A Survey on MANET Intrusion Detection. *International Journal of Computer Science and Security, 2*(1), 1-11.

Menaria, S., Valiveti, S., & Kotecha, K. (2010). Comparative study of Distributed Intrusion Detection in Ad-hoc Networks. *International Journal of Computer Applications, 8*(9), 11-16.

Nadeem, A., & Howarth, M. (2009). *Adaptive intrusion detection and prevention of denial of service attacks in*

MANETs. International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, Leipzig, Germany, pp. 926-930.

Nakayama, H., Kurosawa, S., Jamalipour, A., Nemoto, Y., & Kato, N. (2009). A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks. *Vehicular Technology, IEEE Transactions on, 58*(5), 2471-2481.

Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad Hoc On-Demand Distance Vector (AODV) Routing.

Ramadas, M., Ostermann, S., & Tjaden, B. (2003). *Detecting anomalous network traffic with self-organizing maps*. Recent advances in intrusion detection, RAID. Lecture notes in computer science (LNCS), 2820, 36-54.

Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H., & Zhou, S. (2002). *Specification-based anomaly detection: a new approach for detecting network intrusions.* Proceedings of the Ninth ACM Conference on Computer and Communications Security, pp. 265-274. http://dx.doi.org/10.1145/586110.586146

Stamouli, I. (2003). Real-time Intrusion Detection for Ad hoc Networks.

Sun, B., Wu, K., & Pooch, U. W. (2003). *Alert Aggregation in Mobile Ad Hoc Networks.* The 2003 ACM Workshop on Wireless Security in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78.

Ye, N., Emran, S. M., Chen, Q., & Vilbert, S. (2002). Multivariate statistical analysis of audit trails for host-based intrusion detection. *IEEE Transactions on Computers, 51*(7), 810-820. http://dx.doi.org/10.1109/TC.2002.1017701

Yeung, D. Y., & Ding, Y. (2003). Host-based intrusion detection using dynamic and static behavioral models. *Pattern Recognition, 36*(1), 229-243. http://dx.doi.org/10.1016/S0031-3203(02)00026-2

Yi-an, H., & Wenke, L. (2003). *A Cooperative Intrusion Detection System for Ad Hoc Networks.* Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03).

Zhang, Y., & Lee, W. (2000). *Intrusion detection in wireless ad-hoc networks.* The 6th Annual International Conference on Mobile Computing and Networking, pp. 275-283.

Zhang, Y., Lee, W., & Huang, Y. (2003). Intrusion Detection Techniques for Mobile Wireless Networks. *Wireless Networks Journal (ACM WINET), 9*(5), 545-556. http://dx.doi.org/10.1023/A:1024600519144