International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 4– No.10, December 2012 – www.ijais.org

IDSs based on Stand-alone Architecture for MANET: A Survey

Kapil Dhamecha,
Department of Computer Science, Rollwala Computer Center, Gujarat University, Ahmedabad, India

Rutvik Upadhyay,
Department of Computer Science, Rollwala Computer Center, Gujarat University, Ahmedabad, India

Bhushan Trivedi,PhD.
GLS Institute of Computer Technology, Ahmedabad, India.

ABSTRACT

Mobile Ad Hoc Networks (MANETs) are susceptible to a variety of attacks that threaten their operation and the provided services. Intrusion Detection Systems (IDSs) may act as defensive mechanisms, since they monitor network activities in order to detect malicious actions performed by intruders, and then initiate the appropriate countermeasures. IDSs for MANETs have attracted much attention recently and thus, there are many publications that propose new IDS solutions or improvements to the existing. Current IDSs pose challenges on not only capricious intrusion categories, but also huge computational power. Though there are a number of existing literatures to IDS issues, an attempt is made to give a more elaborate image for a comprehensive review on IDSs based on stand-alone architecture for MANETs, because of the uniqueness to identify the attack solely. In addition, the table and the figure summarized in the content contribute to easily grasp the overall picture of stand-alone IDSs along with existing open issues.

Keywords

Mobile Adhoc Network (MANET), Intrusion Detection System (IDS), stand-alone architecture.

1. Introduction

A mobile ad hoc network (MANET) is a collection of autonomous nodes that form a dynamic, purpose-specific, multi-hop radio network in a decentralized fashion. The main advantage is flexibility, adaptability, eased cooperation and efficient communication in environments without the help of any fixed infrastructure or centralized management point. Despite the many advantages, MANETs are inherently vulnerable to various attacks due to some features such as open medium, dynamic topology, lack of centralized management and control points etc. [18].An effective way to identify an attack occurs in a MANET is the deployment of an Intrusion Detection System (IDS). The IDS is introduced to detect possible violations of a security policy by monitoring system activities and responding to those that are apparently intrusive. It also provides information about intrusion techniques, enhancing the understanding of attacks and informing the decisions regarding prevention and mitigation.

IDS can be categorized using three different ways [4, 17]:

(i) **Based on the architecture**, which exemplifies the operational structure of the IDS ;
(ii) **Based on detection engine**, which is the mechanism used to detect malicious behaviors;
(iii) **Based on data collection technique**, which is the mechanism used to collect and intercept data.

IDS for MANETs have attracted much attention recently and thus, there are many publications that propose new IDS solutions or improvements to the existing IDSs, focusing on IDS architectures. The existing IDS architectures for MANETs fall under four basic categories [4, 16]:

a) ***The stand-alone architectures***use an intrusion detection engine installed on each node utilizing only the node's local audit data.

b) ***The distributed and cooperative architectures***include an intrusion detection engine installed on every node, which monitors local audit data and exchanges audit data and/or detection outcomes with neighboring nodes in order to resolve inconclusive detections.

c) ***Thehierarchical architectures***amount to a multilayer approach, by dividing the network into clusters. Specific nodes are selected (based on specific criteria) to act as cluster heads and undertake various responsibilities and roles in intrusion detection that are usually different from those of the simple cluster members.

d) The Mobile Agent based architectures 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.
The figure 1 in Appendix A shows the classification of IDS based on above discussion and different approaches for the stand-alone architecture.

This paper focuses on IDSs based on stand-alone architecture for MANETs for several reasons. The stand-alone IDS architecture does not incur any communication overhead, since no cooperation between nodes takes place except routing protocol. On the other hand, distributed and cooperative architecture requires nodes to exchange alerts, audit data, and detection results that impose extra communication overheadto the underlying network. Also the impact of nodes' mobilityon detection accuracyand rate of false positives are less in stand-alone architecture [5].

The distributed and cooperative approach imposes an *extraprocessing* workload at each node as detection is carried out at local and global level [5]. On the other hand, in stand-alone architecture detection is carried out only locally.

The hierarchical architectures impose unfair workload distribution among the network nodes,since the nodes elected as cluster-heads are overloaded with detection responsibilities in accordance with reelections of the cluster heads. On the other hand, in stand-alone architecture each node comprises same workload as each node has the same detection engine installed independently.

For Mobile Agent based architectures each agent migrates from one host to another taking the code, data and state with them. This as a whole reduces network bandwidth. It decreases the computation overhead in each node in the network [6]. However, it imposes extra communication overhead as mobile agent needs to be migrated among the nodes. On the other hand, the stand-alone architecture does not require the detection engine to be migrated.

The rest of this article is organized as follows. Section 2 shows the related work for different existing stand-alone IDSs. Section 3 describes the comparison criteria for each stand-alone IDSs focusing on their implementation environments, performance parameters, addressed attacks and open issues. Finally, section 4 contains theconclusions and proposes some suggestions for future research.

2. RELATED WORK

In stand-alone architecture, an intrusion detection system runs on each node independently to determine intrusions. Every decision made is based only on information collected at its own node, since there is no cooperation among nodes in the network. Besides, nodes in the same network do not know anything about the situation on other nodes in the network, as no alert information is passed.

A very first approach to stand-alone architecture proposed by Bansal and Baker (2003) [14] is an extension on top of the DSR protocol called **OCEAN** (Observation-based Cooperation Enforcement in Adhoc Networks).The objective of this approach is to avoid trust-management using a monitoring system and a reputation system for neighbor node's behavior. OCEAN considers two types of routing misbehavior: misleading and selfish behavior using faulty threshold and chip counts mechanisms.

Nadkarni and Mishra (2004) [8] proposed a **Threshold Based** stand-alone IDS architecture that uses compound detection aiming at reducing the amount of false positive alerts, which typically appear in anomaly detection. It employs adjusting thresholds to determine malicious behaviors based on the initial normalized profile.

S Gavini (2004) [10] presented an anomaly based **Unobtrusive Monitoring**technique which relies on readily available information such as DSR Route Error messages, TCP timeout and retransmission time to detect the presence of malicious nodes.

Jacoby and Davis (2007) [7] proposed a **Battery Based** stand-alone architecture for detecting malicious actions in MANETs by monitoring power consumption in every node's battery. Detection is achieved by comparing a node's power consumption with a set of power consumption patterns induced by known attacks, using smart battery technology.

Nakayama et al. (2009) [13] proposed a **Dynamic Anomaly Based** detection system to detect malicious activities that target at the AODV routing protocol. This approach uses the machine learning technique in order to generate and maintain a normal profile and relies on principal component analysis (PCA) for resolving malicious behaviors.

Lauf et al. (2010) [9] proposed a **Two Staged**, stand-alone IDS architecture which is a combination of two detection engines, known as HybrIDS. The first one is an anomaly detection engine that identifies statistical oddities in the observed interactions of the application layer. If a possible attack is identified, a second engine is activated that calibrates a threshold value considering the attack. Then, calculates average values of the application behavior of every node and compares them with the threshold.

Kabiri and Aghaei (2011) [11] presented an anomaly-based **Feature Analysis** technique that focuses on denial of service attacks. The proposed system gets benefit from its neighbors' normal behaviors and analyzes them based on the optimal features. This approach is based on feature selection method and it applies Principal Component Analysis (PCA) theory to determine network operating conditions.

Joseph et al. (2011) [12] proposed a **Cross Layer** detectionof sinking behavior, which hold themachine learning algorithms to detect sinking attacks. The features arecollected from network layer, MAC and physical layer. SVM (Support Vector Machines) is a nonlinear classifier which is used to train the detection model. The directions of SVM margins and the FDA's linear hyper plane are compared and validated, which is used to derive a function for real time detection of the malicious behavior.

3. COMPARISON CRITERIA

This section focuses on different performance parameters, implementation environment, addressed attacks and open issues as the comparison criteria for each stand-alone IDS, which is then summarized in Table 1 (Appendix B).

3.1 Implementation Environment

To measure and validate the effectiveness of any approach, the implementation environment is an essential criterion to the detection mechanism under the different network scenarios.

In **OCEAN [14]**, authors have evaluated the proposed approach based on *Glomosim* network simulator with 40 nodes and 20 m/s velocity. The first test is based on the throughput of cooperating nodes, in the presence of varying numbers of misleading nodes subjected to the network with and without the OCEAN. The 2nd test shows the comparison of the OCEAN and the SEC-HAND across varying values of the faulty threshold and varying degrees of mobility. The performance of the OCEAN and the SEC-HAND in the face of transient failures and rushing attack is evaluated using 3rd and 4th test respectively.

On a **Threshold Based [8]** stand-alone IDS architecture, the simulation test bed in *NS-2* simulator is based on a 670 x 670

meter flat spaces with 50 mobile nodes and a random way point mobility model. Simulation is carried out for DoS attack (detection accuracy), Replay attack (false positive ratio) and Compromised nodes attack (packet delivery ratio, the average end-to-end delay), while varying the node mobility, node density (by varying the movement space from 670x670 to 837x837 while keeping the number of nodes same) and the number of malicious nodes in the network.

The **Unobtrusive Monitoring [10]**based IDS is simulated using *NS-2* under different mobility models (Random Way-Point Model, Gauss-Markov Model, Reference Point Group Mobility Model, City Section Mobility Model) on a network with 50 nodes in the flat 670m X 670m topography. Each simulation is run for a time period of 150 seconds along with performance parameters mainly focusing on the detection interval.

As the **Battery based [7]** IDS is having three different monitoring modules, authors have tested each module separately with real time analysis. As the HIDE identifies the battery power irregularities, the testing range is 20-25 degree Celsius temperature. Windows CE OS keeps track of every open port by storing the relevant information in the memory. By accessing this information, SPIE can be used to show which ports are open. Data collection for HASTE requires an oscilloscope to obtain accurate sets of instantaneous battery current at high sample rates.

In **Dynamic Anomaly Based [13]** IDS, the authors have simulated the proposed approach using *NS-2*. This approach addresses mainly the message forging attacks and the malicious flooding attacks. The simulations are performed for the following two scenarios: (1) a 50-node network with a network topology of 1000 m × 1000 m, (2) a 100-node network with a network topology of 2000 m × 2000 m. Then the comparison is made based on three ways of using the training data sets: initial training dataset, most recent training dataset and adaptive learning dataset.

In **Two Staged [9]** IDS, first, a static set of behaviors is determined offline, and these behaviors are tracked dynamically during the operation of the network with the combination of MDS and CCDS detection engines. The testing of this approach is performed on the small scaled embedded devices. Data generation is performed in a *MATLAB* script that simulated the mission data based on a probability density function, with two real time scenarios of ADS- B and Massively Distributed Micro robotics.

The performance of the **Feature Analysis based [11]** stand-alone IDS is carried out using the simulation with different network conditions and DoS attack scenarios. A logger function is added to the DSR protocol to log the feature values with sampling rate of 1 second. The different network conditions are created using different traffic densities (far - close), node's mobility (fast-static-slow) and no. of nodes (scaling, 20-50) over the area of 2000x2000 m and 250 m of radio range. The results show that the selected parameters (like no. of RREQs, no. of RREPs, no. of sent packets and the time stamps) highly deviate under the attacks.

The **Cross Layer [12]** based IDS is simulated using *Qualnet 3.5* over an area of 1500x1000 m. The node transmission range is set to 250 m and no of nodes is set to 50 with random way point mobility model. For performance brevity, only three factors, mobility, traffic density, and drop ratio, are considered and varied to create different network scenarios. The results are compared between cross-layer SVM (aided by the FDA), cross-layer FDA, and single-layer SVM (aided by the FDA).

3.2 Processing Overhead

The processing overhead refers to the type of detection engine and the algorithms utilized. They are responsible for data collection to find anomaly from available data. The more complex algorithm will incur higher processing power, higher detection time, and more battery power, which are the constraints for IDSs in MANET.

The **OCEAN [14]** is less complex, incurs less processing overhead, as it eliminates trust management complexity using faulty threshold and chip counts mechanisms.

In **Threshold Based [8]** IDS, audit data analysis of network information along with Threshold Analysis Module to adapt network behavior by varying the threshold to identify attacks, incurs some processing overhead.

The **Unobtrusive Monitoring [10]**based IDSincludes a detection algorithm, which is less complex as only routing protocol error messages, TCP timeouts and retransmission times are utilized to identify the anomaly in routing protocols, incurs less processing overhead.

In **Battery Based [7]** stand-alone IDS, the processing overhead is higher since the power signatures captured by HIDE are processed with FFT and chi square test to find close attack signatures, which arethen, compared with known attack signatures by HASTE. Also the SPIE needs to ascertain the IP and port source of the attack.

Because of adaptive learning processing in **Dynamic Anomaly Detection Based [13]** IDS the complexity of the algorithm is higher which incurs higher power and processing overhead.

Despite of two detection engines the HyberIDS of **Two Staged [9]** IDS performs well and incurs lessprocessing overhead by using situational awareness to reduce the need for large and complex computations.

The **Feature analysis Based [11]** approach intends to reduce the dimensionality of the network features using PCA and covariance matrix which incur less processing overhead.

In **Cross Layer [12]** detection based IDS, processing overhead is higher, which includes computational complexity of both periodic retraining of the SVM base model and the detection complexity of the kernel function. Besides, the numbers of features are reduced using data reduction techniques.

3.3 Detection Accuracy

This determines the rate of attacks detected correctly by IDS in a given environment during a particular time frame.
This also includes the rate of false positives or negatives. A false positive is an alert caused by normal non-malicious

background traffic. A false negative is means failure of IDS to detect the actual attack.

The **OCEAN [14]** possesses highdetection accuracy at moderate mobility, and low rate of the false positives even at high faulty threshold.

The **Threshold Based [8]** IDS possesses highdetection accuracy (Avg. 90%) and less false positives, as varying threshold adopts network changes quickly to each of the addressed attacks.

The **Unobtrusive Monitoring Based [10]** IDS possesses highdetection accuracy and lowfalse positives over a wide variety of mobility models.

The **Battery Based [7]** based IDS possess very high detection accuracy (99%) for the known attack signatures but only one at a time.

The **Dynamic Anomaly Detection [13]** based IDS possesses high accuracy and low rate of the false positives because of the adaptive nature of anomaly based engine, which quickly learns the network changes.

Employing two detection engines at each node, increases detection accuracy in **Two Staged [9]** IDS compared to single engine IDSs, since the one engine supplements the other.

Feature Analysis Based [11] IDS possesses high detection accuracy, since the normal profile is derived based on the features which show less variations with respect to the network traffic type, density and other network parameters, that have varying values.

In **Cross Layer [12]** IDS, the kernel function is derived using the directions of SVM margins and the FDA's linear hyper plane, incurs very highdetection accuracy.

3.4 Impact of Node's Mobility

Mobility makes the routes dynamic, i.e., an active route can become broken due to mobility. Here, the dropping of the packets becomes inevitable, as reestablishing a new route takes some time. Furthermore, mobility creates a changing channel and fading conditions [12].

Increasing the mobility of the nodein **OCEAN [14]** decreasesthe detection accuracy as it is more sensitive to the tuning of the Faulty threshold parameter**.** High mobilityincreasesthe rate of false positives.

In **Threshold Based [8]** IDS, increasing the mobility of the nodeaffects very less on detection accuracy and rate of false positives.

Increasing the mobility of the nodedecreasesthe detection accuracy and increases the rate of false positives in **Unobtrusive Monitoring Based [10]** IDS.

In **Dynamic Anomaly Detection [13]** based IDS,an increase in the mobility of the node decreasesthe detection accuracy and *i*ncreases the rate of false positives.

High mobility of the node and the traffic density does not affect the detection accuracy and the rate of false positives in **Feature Analysis Based [11]** IDS, since the response of the system shows same deviations for the selected parameters.

In **Cross Layer [12]** IDS, high mobility makes a negligible drop (less than 1% hence negligible) in detection accuracy and the rate of false positives.

3.5 Traffic / Node Density

Network traffic density or the node density is a crucial factor. They determine how dense the background activities and interference, which will aid in camouflaging malicious behaviors. This affects the detection efficiency [12].
Increasing the node density in**Threshold Based [8]**slightly decreases the detection accuracy and increases average end-to-end delay at the initial time.

Network traffic density does not affect the detection accuracy and false positives in **Feature Analysis Based [11]** IDS.

In **Cross Layer [12]** IDS, cross-layer methods experience *a* negligible drop in detection efficiency while traffic density increases.

3.6 Detection Interval

Detection interval specifies the duration within which a source node keeps track of all the control messages received at that node. The detection interval means that a node has to store information for a longer period of time. If the node is receiving a lot of messages, this can drastically increase the storage overhead which is a burden on the memory constrained mobile nodes. Therefore, the choice of the detection interval has a very significant impact on the performance of IDS [10].

However, only the **Unobtrusive Monitoring Based [10]** IDS signifies the detection interval. Increasing the detection interval lowers the detection effectiveness and lowers the number of false positives and vice versa.

3.7 Scalability

An important aspect of the IDS is its ability to scale to larger networks. Adding more nodes to the ad-hoc network should minimally impact the efficiency of the IDS [9].

Scaling up the network increases the rate of false positives in **Dynamic anomaly Detection [13]** basedIDS.

In **Two Staged [9]** IDS, scaling up the network does not affect detection accuracy.

Also, scaling up the network does not affect the detection accuracy in **Feature Analysis Based [11]** IDS.

3.8 Addressed Attacks

Detecting Intrusion is difficult, particularly in the wireless domain. IDS often attempts to differentiate abnormal activities from the normal ones. Unfortunately, normal activities can be varied, and an attack may have resemblance to normal activities. For any IDS, the ability to identify the type of attacks is the most attractive feature.

The **OCEAN [14]** can identify routing behavior attack, resource utilization attack and rushing attack.

The **Threshold based [8]** IDS addresses DoS attack, replay attack and compromised nodes.

The **Unobtrusive Monitoring Based [10]** IDS can identify the misbehaving nodes, malicious packet dropping nodes and Byzantine attack.

The **Battery Based [7]** IDS has an ability to provide timely detection for DoS attacks (Dirty dozens) and for those who causes power anomalies.

The **Dynamic Anomaly Detection [13]**can detect routing disruption attacks malicious flooding and packets dropping misbehavior.

The **Two Staged [9]** can identify a DoS (Jamming), spoofing and mislead attacks.

The **Feature Analysis Based [11]** IDS can identify DoS attacks at MAC and network layers promiscuously.

The **Cross Layer [12]** detection based IDS identifies sinking attacks such as selective dropping and sinkhole attack.

3.9 Open Issues

Even if some of the described IDSs do well towards securing the MANET, enhancing solutions are required to their limitations and weaknesses, which constitute open issues that will drive the next steps in the research area of MANET security. The study reveals that many gaps still exist for detecting intrusions.

In **OCEAN [14],** the performance falls drastically for low number of misleading nodes. It is more sensitive to some parameter settings and does not punish misbehaving nodes as severely as systems using full-blown reputationinformation. Also, it is not effective in thwarting the throughput of misleading nodes. The authentication mechanism is also required to avoid spoofing of legitimate node's identity.

Adjustable threshold creates new weaknesses as malicious node can still fool the **Threshold based [8]** IDS by varying its behavior smartly. Also coordinated attacks (i.e., such as Byzantine attacks) cannot be detected, since nodes do not cooperate.

The **Unobtrusive Monitoring Based [10]** IDS cannot distinguish packet drops due to congestion and malicious behavior. Also, collaborative attacks (such as Byzantine attack) cannot be identified.

In **Battery Based [7]** IDS, it is difficult to obtain battery current readings at higher sample rates with the current technology. It also sustains an inability to analyze every type of network protocol, as not every network protocol allows raw sockets in promiscuous mode. It can detect only attacks that cause power irregularities and only in cases that the nodes are idle, something that rarely occurs in real systems.

The **Dynamic Anomaly Detection [13]** based IDS cannot be used for detection of all possible attacks as it cannot detect collaborative and DoS attacks.

The **Two Staged [9]** IDS is prone to false positives and negatives, since it calibrates the threshold value only once during startup. Also, it cannot identify routing attacks.

The **Feature Analysis Based [11]** IDS addresses only DoS attacks.

The **Cross Layer [12]** IDS identifies only sinking attacks.

4.CONCLUSION &FUTURE DIRECTION

This paper evaluates and compares the latest and most prominent stand-alone IDS architectures for MANETs along with performance aspects and present significant limitations.
Also, Table 1 (Appendix A) shows, much of the stand-alone architectures can identify a limited set of attacks due to lack of cooperation and failed to identify coordinated attacks. Some of the evaluated IDS architectures cannot detect all types of attacks [7,11,12], since they focus only on specific types of intrusions.The number of new attacks is likely to increase quickly and those attacks should be detected before they can do any harm to the systems or data. Hence, IDS's in MANETs prefer using anomaly detection. Most approaches are proposed to implement on top of the existing protocols [10,11,12, and13]. Most of the above described IDSs are simulated[8, 10, 11, 12, and 13]. The processing overhead in most of the IDSs is less[9, 10, 11, and 14]. However, the impact of nodes' mobility and density decrease the detection accuracy in most of the stand-alone IDSs[8, 10, 12, 13, and 14]. The impact of detection interval, the most essential parameter for the performance of any IDS, is not even addressed by any of the described IDSs except[10].
However, out of them Feature Analysis Based IDS [11] is the most promising candidate because of high detection accuracy andless computational overhead. The salient feature of the IDS is it has no effect on traffic density and nodes' mobility. However, it only addresses the DoS attacks and considers the DSR routing protocol.
The future direction includes expansion of the feature analysis approach that can focus on other routing and misbehaving attacks such that the approach would be the best fitted. Also the approach can be made protocol independent so that it can be deployed over a wide area.

5. REFERENCES

[1] H. Miranda and L. Rodrigues, 'Preventing selfishness in open mobile ad hoc networks,' in Proc. Of the Seventh CaberNet Radicals Workshop, October 2002.

[2] D. Djenouri, L. Khelladi, N. Badache, "A Survey of Security Issues in Mobile Ad Hoc Networks," IEEE Communications Surveys, Vol. 7, No. 4, Fourth Quarter 2005.

[3] S. Sen and J. A. Clark, "Intrusion Detection in Mobile Ad Hoc Networks". In: Guide to Wireless Ad Hoc Networks, S. Misra, I. Woungang, S.C. Misra (Eds.), Springer, 2009.

[4] T. Anantvalee, J. Wu, "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, Chapter 7, pp. 170 - 196, 2006.

[5] C. Xenakis, C. Panos, I. Stavrakaki,"A Comparative Evaluation of Intrusion Detection Architectures for Mobile Ad Hoc Networks" Computers and Security , Elsevier, pp. 63-80,2011.

[6] Y. Jain, R. Ahirwar,"Secure Mobile Agent Based IDS for MANET", International Journal of Computer Science and Information Technologies, Vol. 3 (4), pp. 4798-4805, 2012.

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

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

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

[10] S. Gavini," Detecting Packet dropping faults in Mobile Adhoc Networks", 2004.

[11] P. Kabiri, M. Again, "Feature Analysis for Intrusion Detection in Mobile Ad Hoc Networks",International Journal of Network Security, 12 (2), 80-87, 2011.

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

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

[14] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks," Research Report cs.NI/0307012, Stanford University, 2003.

[15] S. Srivastava, N. Gupta, S. Chturvedi, S. Ghosh, "A Survey on Mobile Agent based Intrusion Detection System", ISDMISC, IJCA, 2011.

[16] D Kheyri1 & M Karami1,"A Comprehensive Survey on Anomaly-Based Intrusion Detection in MANET", Computer and Information Science; Vol. 5, No. 4; 2012.

[17] Y Huang, & L Wenke," *A Cooperative Intrusion Detection System for Ad Hoc Networks",* proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks2003.

Appendix A:

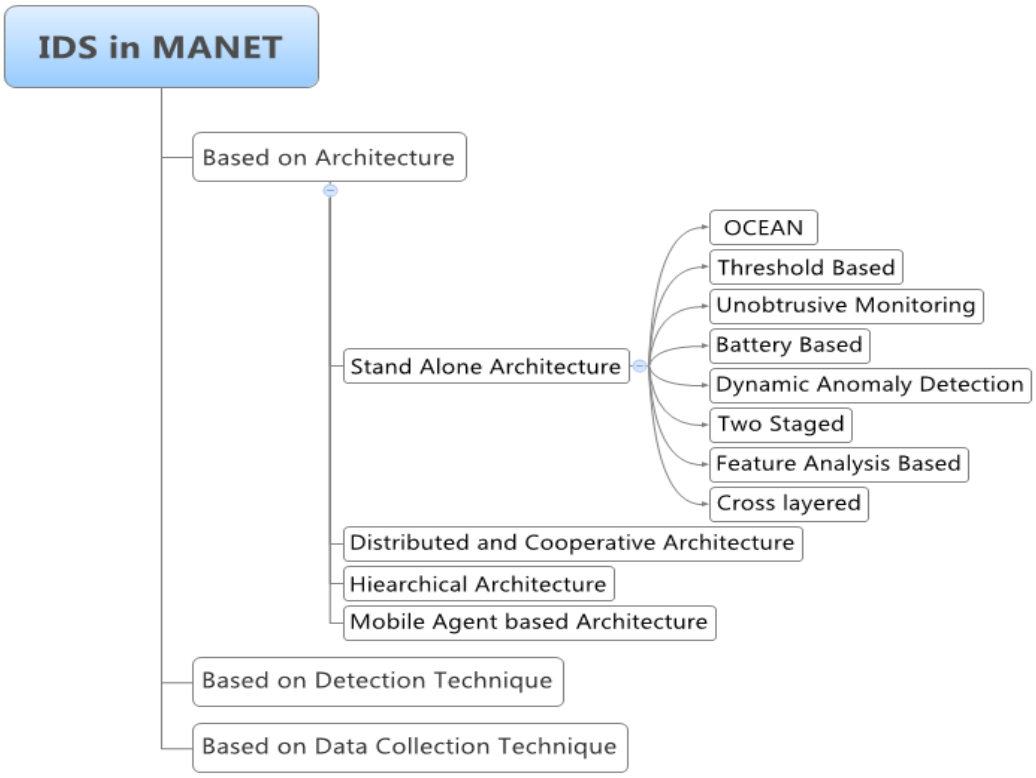

Figure1: Classification of IDSs and different approaches for Stand Alone Architecture

Appendix B:

Table 1: Comparison of stand-alone architecture based intrusion detection systems

IDS	OCEAN [14]	Threshold Based [8]	Unobtrusive monitoring based [10]	Battery Based [7]	Dynamic Anomaly Detection [13]	Two Staged [9]	Feature Analysis Based [11]	Cross Layer [12]
Routing Protocol	Not specified	Protocol independent	DSR	Not specified	AODV	Not Specified	DSR	OLSR
Detection engine	Anomaly	Anomaly + Misuse	Anomaly	Specification + Misuse	Anomaly	Anomaly	Anomaly	Anomaly
Implementation environment	Simulation	Simulation	Simulation	Real time	Simulation	Real time	Simulation	Simulation
Processing overhead	Low	Moderate	Low	High	High	Low	Low	High
Detection accuracy	Very high	High	High	High	High	High	High	Very High
Impacts of node's high mobility	Decreases accuracy + Increases false positives	Affects very less to detection accuracy and false positives	Decreases accuracy + Increases false positives	N/A	Decreases accuracy + Increases false positives	N/A	Does not affect the accuracy and false positives	Negligible drop in detection accuracy and false positives
Impact of Traffic/Node density	N/A	Slightly affects the detection accuracy + Increases end delay	N/A	N/A	N/A	N/A	Does not affect the accuracy and false positives	Negligible drop in detection efficiency as traffic density increases
Impact of node's Detection Interval	N/A	N/A	High interval lowers the accuracy +lowers false positives and vice versa.	N/A	N/A	N/A	N/A	N/A
Scalability	N/A	N/A	N/A	N/A	Increases the rate of false positives	Does not affect detection accuracy	Does not affect detection accuracy	N/A
Attacks Addressed	Routing behavior attack, Resource utilization attack and Rushing attacks	DoS attack, Replay attack and compromised nodes	Misbehaving nodes, malicious packet dropping nodes and Byzantine attack	DoS attacks (Dirty dozens) and those causes power anomalies	Route disruption malicious flooding, Packets dropping misbehaviors	DoS attack (Jamming), spoofing and mislead attacks	DoS attacks	Identifies only sinking attacks