# A State of an Art Survey of Intrusion Detection System in Mobile Ad-hoc Network

Devendra Singh
IFTM University, Moradabad, India

S.S. Bedi
MJP Rohilkhand University, Bareilly, India

## ABSTRACT
Mobile Ad Hoc Networks are more vulnerable to attacks. Due to vulnerability, security in MANETs has been an issue of prime importance in the recent years. The common attack prevention techniques such as cryptographic techniques (Authentication/Digital Signatures) cannot be implemented in MANETs as there is no central controlling device for authentication. This necessitates the need for some other security mechanisms to prevent/detect various types of attacks in MANETs. One such mechanism is to implement Intrusion Detection System. Intrusion Detection System (IDS) has been widely studied in the past and continues to be focus of research in the recent years.

This paper summarizes the most prominent IDS Architectures for MANETs published in the last five years. The summary includes brief descriptions of IDS architecture, IDS Techniques (Detection Engines), Types of Attacks detected and Data gathering techniques, followed by the author's comments on strength, weaknesses and limitations of each technique. Further, a comprehensive table is presented including all summarized papers, at a glance, lists salient features and author's comments for each technique to facilitate new researchers to select a specific area for their work.

## Keywords
MANET (Mobile Ad hoc networks), IDS (Intrusion Detection System), AODV (Ad hoc On-demand Distance Vector), DSR (Dynamic Source Routing), NS2 (Network Simulator2).

## 1. INTRODUCTION
Ad Hoc Networks is used to rapid deployment of a network on the urgent temporary basis or for the specific purposes such as disaster, military battle field etc. due to this rapid deployment, MANET has limited resources (such as lack of infrastructure, limited battery power) and make it more vulnerable to attacks. In MANETs all active and passive attacks can reduce the performance of networks which was present in wired networks in addition to these attacks MANET have rise some new attacks e.g. Blackhole, routing loop, network partition, selfish node, sleep deprivation. So to overcome this problem needs some security mechanism. Intrusion Detection is one of security mechanism. Because of lack of central controlling or a point of controlling we cannot implement cryptographic techniques such as key distribution or certification authority to provide the authentication or providing digital signatures to the individual node(s). Firewall and other cryptographic techniques are used to detect or handle with external attacks called first line of defense to network system such prevention methods is not possible to deploy in MANET. Therefore, need another solution to mitigate the attacks i.e. Intrusion detection System, which observe the network traffic/activities and can handle with internal as well as external attacks and thus it is called second line of defense. IDS is not a new area, it has been an active research area for over three decades, due to the characteristics of MANET traditional IDS cannot be directly apply to MANETs special mechanism to deploy IDS in MANETs [1]. In ad hoc network a node can monitor the traffic packet or collect the information about the network traffic only in its transmission range. MANETs divides into two types (i) open ad hoc means no prior security (ii) close ad hoc means prior security installed. Intrusion Detection is a system which can detect attacks in both types of networks automatically. Commonly, IDS works on three modules, these are collection/monitoring of information, detection and response [2]. Firstly, collection of data or monitoring is done through all or selected nodes in the networks at packet level, user level, network level and application logs. Secondly, detection processes is done through some detection engines/techniques viz. anomaly, misuse and specification based. Lastly, third one is response process, which detected node sends an alert message to all the benign nodes. IDS are basically classifying two types IDS Architecture and Detection Techniques. IDS Architecture is based on the logically organization of node(s) in the network. Detection Techniques is the mechanism to detect the malicious behavior(s) in the network. The existing IDS architectures for MANETs fall under four basic categories [2,3]: Stand Alone IDS, Cooperative and Distributed IDS, Hierarchical IDs and Mobile Agent based IDS.

On the basis of detection techniques used in IDS. IDS detection techniques can classify into three main categories: Anomaly Detection, Signature or misuse based IDS and Specification based IDS.

Anomaly Detection used a predefined normal behavior, if the behavior deviates from predefined expected behavior then it detects as abnormal. Anomaly detection does not require database for existing attacks for this reason it is widely used in the MANETs. It can detect novel attacks based on predefined conditions but it causes very high false positives.

Misuse or Signature based detection uses predefined patterns of attacks, which matches to the patterns and identifies the attacks. For matching the patterns it needs databases to store patterns or signature of attacks. Due to this reason it detects the existing attacks very speedy and accurately but it fails to detect new attacks not defined in the database.

Specification based detection observed the current behavior of systems to the defined operation of the protocol/program called specification, if system operation deviates from these specifications then it get malicious.

IDS is very popular research area, thus there are many papers considering both architecture and detection techniques have been published that proposes the improvements in existing or new solutions to IDS. Beside that some work has been done on comparing and evaluating them to present that strength and weaknesses. Satria Mandala et al [2] have presented a survey of MANET and detection techniques. They include all the papers before 2006 and conclude that most of the researches worked on cooperative and hierarchical architectures. Christos

Xenakis et al [4] have presented a comparative evaluation of IDS architecture and present the strength and weaknesses of architectures and present the set of design feature and principles. Similarly, Navoron et al [5] have presented a survey for IDS in MANET and WSN they include all the papers before 2010 and concluded that a scalable architecture is needed to implement IDS in MANET.

In this paper, well known IDS architectures, detection engines and implementing techniques to a particular architecture is compared. Which signify the current developments in this area. Brief literature survey of each paper that have been considered for our work then a comparative analysis with the help of table of each papers that taken into literature survey and then finally, combined analysis of literature on the basis of comments in the comparative analysis. In the combined analysis, find some suitable guidelines to make a robust IDS system to mitigate the attacks and have optimized performance in various situations. This paper will help for those people who are looking into field of security in MANETs. Author's comments about the strength and weaknesses on the basis of IDS architecture and detection engines and types of detected attacks.

Some of the main factors which effects IDS performance in MANETs are mobility speed of nodes, type of architecture, type of routing protocol, detection engines used, which are mainly to classify among the friend node and the malicious node.

In this paper, various recent papers have been studied. Remaining paper is organized as follows. Sections 2 contain the literature survey of the most recent IDS with comparative analysis on the basis of factors which affect the performance of IDS. Section 3 briefly explains the guidelines to select the IDS and lastly section 4 describe the conclusion and future work.

# 2. RELATED WORK

## 2.1 Survey of architecture and detection engines

### *2.1.1 Standalone Architecture*

In this architecture IDS detects the attacks at each node using local audit data. Some most recent local IDS architecture in MANETs is presented.

In reference [7][8], authors uses the misuse detection (knowledge based) system. Depending on type of attacks particular rules are used to detect the attacks. They implement AODV routing protocol in NS2 to analyses network traffic. EIDAN uses local intrusion detection system and implement on each node of the network. Authors detect only malicious packets in the network traffic but they could not find the malicious node. Response module is not implemented.

According to reference [9], authors detect the blackhole attack over AODV. They detect the attacker's node with the help of attacker's previous node locally. They extend the work of H.Deng [10]. Simulation results shows that it is better than SID techniques but this approach will not work correctly in the network where more than one attacker attacks the network.

### *2.1.2 Cooperative Intrusion Detection*

In this architecture each node collects audit data with the help of other node and share information among themselves. Detection of attacks is done on some or all nodes of networks. Detection engines may cooperate each other through the results of detection and audit data

In the reference [11], authors tried to find the most critical node, a node where maximum packets are coming and forwarding. It is considered a cut point to the network. mLab test bed is used to find this cut point by implementing a trigger mechanism. This trigger uses the IP header and Ethernet headers of outgoing and incoming packets, which are destined to this critical node.

In the reference [12], a secure routing protocol called SecAODV and IDS have been proposed to finds the malicious node in the network by filtering the packets with the libpcap for capturing packets. They use threshold based detection to find malicious node in the network. In period of congestion, a node may queue packets to be retransmitted instead transmit them immediately, causing the monitor to assume that the packets have been dropped.

In the reference [13], author proposes the IDS for cross layer architecture of IP stack. Different types of attacks at the different layer e.g. routing attack at routing layer, passive attacks at the Physical layer and link resources attacks at data link layer. This Intrusion Detection System detects attack across all the layers. Authors use data mining algorithm which creates feature sets of normal traffic and abnormal traffic with fixed width clustering algorithm. Experimental results shows that the attacker traffic is much more than the normal traffic. They detect DoS and Sinkhole attacks at different layer of protocol stack.

According to reference [14], authors have been proposed a model to detect the intrusions using unfair use of transmission channel detection engine and anomaly detection engine by creating the trusted node list. Detection of transmission channel attacks are predefined, novel attacks for packet type forwarding using anomaly detection engine. Feedback table is also created to the global detection.

According to reference [15], authors have been proposed IDS to detect DDoS by distributing certificates initially so that each node has a directory of certificates. Experimental results shows for three conditions normal time, attack time and IDS time. IDS is implemented at single node only it cannot detect collusion attack.

### *2.1.3 Hierarchical Intrusion Detection*

In this architecture network is divided into groups/Clusters. All cluster member elects their one cluster head which running IDS and detects malicious nodes more accurately.

In the reference [16], authors have been developed a novel intrusion detection system at cluster head based on anomaly detection can work with any other IDS implemented on the cluster member. IDSX maintain a bound table to decide the malicious behavior of the nodes requested by cluster member node. In bound table cluster head records the packets transmission of the suspected node by recording its address and dirty packets and the total packets. If the dirty packet crosses the threshold value then it declares as malicious node.

In the reference [17], authors have been implemented the IDS agents on all the nodes in network but active IDS agent implemented at cluster head. New backup node of cluster head created because cluster head may become selfish. Signature based detection is implemented on cluster head and anomaly detection is implemented on backup node. If cluster head or backup node finds malicious then they demands reelection immediately. They simulate their work in C.

In the reference [18], author extends the work of kim et al. finds the node which has maximum energy by voting in the network. Monitoring module is done by the elected node. Author more emphasizes on the selection of monitoring nodes to enhance network lifetime instead of IDS. Experimental values show that this approach is better than LES.

In the reference [19], D.Sterne at el. has been proposed dynamic hierarchy intrusion detection. A recursive algorithm is used, which makes a tree like three layers of networks. The entire nodes advertise its neighbor and this information stored at cluster heads and distributed to each node. If any node falsely advertises its neighbor it can detect. If cluster head at first level not sure about attack it sends the query to second level and so on. If decision is not sure at second level it then further send to first level i.e. root node where complete information is available to detect attacks. OLSR is used as routing protocol.

In the reference [20], algorithm has been proposed to find the intruder in co-operative manner with the help of voting in the network. But the limitation of this method is that if numbers of node are large in the network then sharing the information among cluster head becomes hectic. They evaluate the performance of node, packet lost and delay graph.

In the reference [21], authors have been proposed a new algorithm based on clustering to find malicious node in the network and alarming others for the presence of malicious node in the network and cut the entire routes through the malicious node in the routing table. The cluster head must be benign node of the network. Authors also give the data structures and tables to stores the information to detect the malicious node.

### *2.1.4 Agent Based Intrusion Detection*

In this architecture agent is used for specific use in IDS mechanism.

In the reference [22], this detects intrusions locally based anomaly model. Feature sets were defined on the basis of packets or routing packets to identify attacks 1SVM method. If the attack is known then it alarm to other nodes otherwise it comes into unknown feature set. They simulate their work in NS2. Mobile agent is used at each node so that all nodes can detect intrusions itself and inform to all other.

In reference [23], the researchers have been proposed the IDS based on the mobile agents deployed at cluster head. Each mobile agent has different purpose to work at cluster head. Intrusion Detection Agent (IDA) is applied on each cluster head, which includes Decision Making Agent (DMA) and Cluster Response Agent (CRA). IDA uses anomaly detection and independently analyses to take decision and send alarm to all cluster members through CRA. Given comparison shows this work is better than other existing techniques.

In reference [24], authors have been proposed Anomaly Intrusion Detection System agent (AIDS) based on Multi-agent Partially Observable Markov Detection Process (MPO-MDP). Moreover, each AIDS sensor is partially known the other sensor information. To minimize communication overhead AIDS sensor detects locally and send the results only to the other sensors. AIDS sensor has the On/Off stages to consume minimum energy and increases the lifetime of network.

In the reference [25], mobile agent based local detection architecture is used. Mobile agent server is fixed at the central point. If mobile nodes is not able to detect any attack locally through signature or anomaly then a mobile agent, which deployed on every node need to confirm or update the signature from mobile agent server. Fixed mobile agent server reduces the mobility of a node.

## 2.2 Comparative Analysis

Comparative Analysis is done with the help of table1, which is given below. In this table various papers on intrusion detection with various techniques, architecture, routing protocols, attacks, detection engines etc. It is necessary to mention here that all the papers which have been reviewed above, have skipped the detection for malicious node or attacks in the network. Further, it is to be emphasized that IDS is dependent on basically two parameters viz intrusion detection architecture and intrusion detection techniques/detection engines. Intrusion detection architectures are local, cooperative, hierarchical and mobile agent based. Architecture of intrusion detection is basically tells us that how node(s) will collect of necessary information and inform other nodes in the overall network. Detection engines are of various types Anomaly, Misuse and Specification based engines. Detection engines used to classify the behavior between normal and abnormal condition or to classify the attacks/intrusions/malicious node(s) on the basis of the available information on node which running the intrusion detection (watchdog , based on pattern recognition like SVM, MSVM, CR4, CR4.5, CR5, neural network. etc). It may be said that selection of parameters in better and synchronized manner, accuracy rate may enhanced, and detection time reduced. It is necessary to mention here, that combination of the various detection engines gives the better results as per above review. However, every architecture has its own limitations such that stand alone Architecture is limited to the detection accuracy because of the limited information available at the local node but beside that it has low communication overhead but in cooperative architecture, detection accuracy is more because of the information is available from all the nodes. Hierarchical architecture has communication overhead is much more higher along with that if mangling of packet attacks cannot detect in this architecture but when the low mobility then it better in detection accuracy because Cluster head acts as the central authority and every communication between nodes going through it. So it is evident from the above study node mobility is very crucial parameter in selecting any IDS solutions.

**Table1: Comparison table**

| S.NO. | IDS architecture/ routing protocol | Detection Engine/ Detected Attacks | Remarks |
|---|---|---|---|
| [7][8] | Stand Alone<br>AODV | Misuse<br>Resource consumption<br>Packet dropping, Fabrication Attack, Seq. no. | Finite State Machine with set of rules, detection accuracy 70-80% in given simulation. EIDAN is extended RIDAN. |
| [9] | Standalone<br>AODV | Anomaly<br>Blackhole attack | LID extends SID. Detects the malicious node at the previous node of attacker node. LID cannot detects colluding attacks. |
| [11] | Cooperative<br>AODV | Detection of Critical node. | IDS on critical node. Critical node may not present in dense network. |
| [12] | Cooperative<br>SecAODV | Anomaly & Misuse<br>Data link and application layer attacks | SecAODV and IDS are complementary to each other. Authentication by implementing certificate authority. Data specifications are stored in lipcap Library |
| [13] | Cooperative<br>AODV | Cross layer Anomaly<br>DDos and Sinkhole attacks | Creating patterns by using fixed width algorithm is time consuming. Collects traffic patterns locally. |
| [14] | Hierarchical | Misuse<br>DDoS | WDBOD is outperform compared with C4,5, SVM, MSVM,ID3. KDD99 Cup dataset is used |
| [15] | Cooperative<br>AODV | Anomaly<br>DDoS | Each node having IDS captures neighbor node information. |
| [16] | Hierarchical | Anomaly detection | Cluster head installed with IDSX. IDSX creates a bound table of dirty packets. IDSX is compatible with other IDS solutions. |
| [17] | Hierarchical | Anomaly and misuse<br>Passive attacks | Back up node of cluster head is proposed. Signature is stored at backup and cluster head node. |
| [19] | Hierarchical<br>OLSR | Anomaly<br>Worm hole<br>False neighbor advertising | Three layers of hierarchy in tree form. Intermediate nodes and root nodes are cluster head. Recursive algorithm is used to create hierarchy |
| [20] | Hierarchical<br>AODV | Anomaly detection<br>Misbehavior attacks | ADCLI algorithm is installed on monitor node. Detection of anomaly is based on the votes of other nodes at monitor node. |
| [21] | Hierarchical | Anomaly detection<br>General attacks | head_malicious, Malicious and Packet_tables are proposed to detect malicious node. Each packet stored in tables |
| [22] | Agent based local detection<br>AODV | Anomaly<br>Blackhole, Flooding disruption | Agent using SVM method to classify the anomalies in given feature sets. |
| [23] | Agent based hierarchical<br>CBRP | Anomaly<br>General attacks | IDA, CRA and NRA agents are used. Threshold based on energy to send and receive. |
| [24] | Agent base Cooperative | Anomaly detection<br>Packet dropping, DoS | AIDS sensor is used with MPO-MDP. Sensor collects link_state, reputation and power observations. |
| [26] | Agent based<br>Local IDS | Anomaly and Misuse<br>DDoS, Routing table poisoning | SNMP Agents are used to collect audit data. Stored collected fetures in MIB. |

## 3. GUIDELINES TO SELECT IDS

Here some guidelines proposed to select the IDS on the basis of the literature survey of studied IDS Architecture and detection engines and operational characteristics, which is derived from the carried analysis in various papers. To make robust IDS in MANET, researchers must take care of these following points. However, it might be possible that single IDS may not cover all these suggestions:

1. Given the nature of MANET, IDS does not become an extra weakness to the network, so every node clearly known their roles in the IDS mechanism.
2. Detection Engines must use some novel techniques like neural network or data mining techniques to classify the attacks at multilayer (i.e. transport, network and data link) otherwise more detection engines are needed to detect attacks at different layer of protocol stack.
3. Mobile agents can be used to minimize the communication traffic by detecting attacks locally and only results passed to other nodes. It is also desirable to use mobile agents in low security environment.
4. In hierarchical architecture network, cluster node send the audit/detected data in the refined form so that only necessary data can reach to the cluster head, instead of voluminous data.
5. Node mobility affects the detection accuracy, produces false alarms and increases the communication.
6. Local detection process is done only after collecting the sufficient data from other node.
7. Alarm must trigger to alert other nodes. So extra information or traffic directed towards this malicious node stops.

## 4. CONCLUSION AND FUTURE WORK

From the above study it is evident that performance of the IDS is dependent on the mobility of nodes, if mobility is high then packet loss is high due to changes in routing information. Due to packet loss detection results will not accurate because of insufficient of information to detect attacks. Moreover, Local detection has low detection accuracy but somewhere works well with mobility factor. Hierarchical architecture is complex in building clusters and reelection procedure due to high mobility in node. Hence cooperative architecture is considered for the further research. Beside the architecture, selection of detection engines is also very important factor. From the above study because of the vulnerability of attacks in MANETs fully dependent on misuse detection type engines is not suitable hence combination of misuse and anomaly detection may be a better approach. From the above study it is infer that the limitation of the misuse detection is to select the feature set and trained the signature. Finally, some of detection engines and architecture cannot detect all types of attacks, since they focus only on specific types of detections attacks.

## 5. REFERENCES

[1] Li, Y and J Wei. Guidelines on Selecting Intrusion Detection Methods in MANET. In The Proceedings of the Information Systems Education Conference 2004, v 21 (Newport): §3233. ISSN: 1542-7382.

[2] Satria Mandala, Md. Asri Ngadi, A. Hanan Abdullah, "A Survey on MANET Intrusion Detection", International Journal of Computer Science and Security, Volume (2): Issue (1). 2008

[3] Kuchaki Rafsanjani, Marjan; Movaghar, Ali; Koroupi, Faroukh:, "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes" Proceedings of World Academy of Science: Engineering & Technolog;Oct2008, Vol. 46, p351

[4] Christos Xenakis, Christoforos Panos, Ioannis Stavrakakis, A comparative evaluation of intrusion detection architectures for mobile ad hoc networks, Computers & Security, Volume 30, Issue 1, January 2011, Pages 63-80, ISSN 0167-4048

[5] A Deb, Novarun, Chakraborty, Manali, Chaki, Nabendu, "A State-of-the-Art Survey on IDS for Mobile Ad-Hoc Networks and Wireless Mesh Networks" Communications in Computer and Information Science P 169-179, 978-3-642-24036-2, P 169-179, 2011

[6] Y. Zhang, W. Lee, and Y. Huang, \Intrusion Detection Techniques for Mobile Wireless Networks," ACM/Kluwer Wireless Networks Journal (ACM WINET), Vol. 9, No. 5, September 2003.

[7] Stamouli, L.; Argyroudis, P.G.; Tewari, H.; , "Real-time intrusion detection for ad hoc networks," World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a , vol., no., pp. 374- 380, 13-16 June 2005

[8] Rajeswari, L. Prema; Annie, R. Arockia Xavier; Kannan, A.; , "Enhanced intrusion detection techniques for mobile ad hoc networks," Information and Communication Technology in Electrical Sciences (ICTES 2007), 2007. ICTES. IET-UK International Conference on , vol., no., pp.1008-1013, 20-22 Dec. 2007

[9] Abdelhaq, M.; Serhan, S.; Alsaqour, R.; Hassan, R.; , "A local intrusion detection routing security over MANET network," Electrical Engineering and Informatics (ICEEI), 2011 International Conference on , vol., no., pp.1-6, 17-19 July 2011

[10] H. Deng, W. Li and D. Agrawal, "Routing security in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp.70-75, 2002.

[11] Karygiannis, A.; Antonakakis, E.; Apostolopoulos, A.; , "Detecting critical nodes for MANET intrusion detection systems," Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006. SecPerU 2006. Second International Workshop on , vol., no., pp.9 pp.-15, 29-29 June 2006

[12] A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis, Y. Yesha, Threshold-based intrusion detection in ad hoc networks and secure AODV, Ad Hoc Networks, Volume 6, Issue 4, June 2008, Pages 578-599, ISSN 1570-8705

[13] Shrestha, R.; Kyong-Heon Han; Dong-You Choi; Seung-Jo Han; , "A Novel Cross Layer Intrusion Detection System in MANET," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.647-654, 20-23 April 2010

[14] Husain, S.; Gupta, S.C.; Chand, M.; Mandoria, H.L.; , "A proposed model for Intrusion Detection System for mobile adhoc network," Computer and Communication

Technology (ICCCT), 2010 International Conference on , vol., no., pp.99-102, 17-19 Sept. 2010

[15] "A SECURE INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORK" M.Vallinayagam, S.Sasikala International Journal of Computer Science and Management Research Vol 1 Issue 4 November 2012

[16] Chaki, R.; Chaki, N.; , "IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad-Hoc Network," Computer Information Systems and Industrial Management Applications, 2007. CISIM '07. 6th International Conference on , vol., no., pp.179-184, 28-30 June 2007

[17] Abhijeet Deodhar and Ritesh Gujrathi "A Cluster Based Intrusion Detection System for Mobile Ad Hoc Networks" 2008.

[18] Chuan-Xiang Ma; Ze-ming Fang; Lei-chun Wang; Qing-Hua Li; , "A Novel Intrusion Detection Architecture for Energy-Constrained Mobile Ad-hoc Networks," Multimedia Information Networking and Security, 2009. MINES '09. International Conference on , vol.2, no., pp.366-369, 18-20 Nov. 2009

[19] Sterne, D.; Lawler, G.; , "A dynamic intrusion detection hierarchy for MANETs," Sarnoff Symposium, 2009. SARNOFF '09. IEEE , vol., no., pp.1-8, March 30 2009-April 1 2009 doi: 10.1109/SARNOF.2009.

[20] Manikandan, T.; Sathyasheela, K.B.; , "Detection of malicious nodes in MANETs," Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on , vol., no., pp.788-793, 7-9 Oct. 2010

[21] Al-Hujailan, H.; Al-Rodhaan, M.; Al-Dhelaan, A.; , "A cooperative intrusion detection scheme for clustered mobile ad hoc networks," Information Assurance and Security (IAS), 2011 7th International Conference on , vol., no., pp.179-185, 5-8 Dec. 2011

[22] Hongmei Deng, Roger Xu, Frank Zhang, Chiman Kwan, Leonard Haynes: Agent-based Distributed Intrusion Detection Methodology for MANETs. Security and Management 2006

[23] B. Pahlevanzadeh, S.A. Hosseini Seno, T.C. Wan, R. Budiarto, Mohammed M. Kadhum "A Cluster-Based Distributed Hierarchical IDS for MANETs" International Conference on Network Applications, Protocols and Services 2008 (NetApps2008) 21 - 22 November 2008 Executive Development Center, Universiti Utara Malaysia.

[24] Zonghua Zhang; Nait-Abdesselam, F.; Djahel, S.; , "ARSoS: An Adaptive, Robust, and Sub-Optimal Strategy for Automated Deployment of Anomaly Detection System in MANETs," Wireless Communications and Mobile Computing Conference, 2008. IWCMC '08. International , vol., no., pp.606-613, 6-8 Aug. 2008

[25] Mechtri, L.; Tolba, F.D.; Ghanemi, S.; , "MASID: Multi-Agent System for Intrusion Detection in MANET," Information Technology: New Generations (ITNG), 2012 Ninth International Conference on , vol., no., pp.65-70, 16-18 April 2012