Comparative Analysis of Architectures for Intrusion Detection Systems against DoS Attacks in MANETs based on Chi-Square Test

A. Anna Lakshmi
ASP / CSE
KSRCE
Tiruchengode
Tamil Nadu

S. Anandkumar
AP / IT
NEC
Erode
Tamil Nadu

G.Nagarajan
AP/CSE
KSRCE
Tiruchengode
Tamil Nadu

K.R.Valluvan,
Ph.D
Professor&Head /ECE
VCET
Erode
Tamil Nadu

ABSTRACT
A Mobile Adhoc Network (MANET) is a group of wireless nodes that can be dynamically organized as a multi-hop packet radio network without using any existing infrastructure or centralized administration. MANETs are susceptible to the variety of attacks that threaten their operation and the provided services. MANET is severely affected by Denial of Service (DoS) attacks which become a problem for internet users. Intrusion Detection System (IDS) may act as defensive mechanism which monitors network activities in order to detect malicious activities performed by intruders and initiate proper response to malicious activity. Several IDS architectures are proposed for detecting the malicious node. In this paper the following IDS architectures for DoS attack in MANET are compared based on Chi-Square test: i)Stand-alone ii)Cooperative iii)Hierarchical iv)Zone based approach using mobile agent. Also listed out the strengths and weaknesses of each IDS architecture. A cluster based cooperative and distributed IDS which uses multiple light weight agents and reduces the overhead of cluster head is proposed. Simulations based on NS2 are as shown.

Keywords
MANET, DoS attack, Intrusion Detection System, IDS architecture, Chi-square test

1. INTRODUCTION
MANET is a collection of autonomous nodes that form a dynamic, purpose-specific, multi-hop radio network in a decentralized fashion. Since MANETs can be installed easily and economically, they have a wide range of applications, especially in Military operations, emergency and disaster relief efforts [1]. Due to the open wireless medium used, dynamic topology, power and computation constraints, distributed and cooperative sharing of channels and other resources[2] MANETs are more vulnerable to variety of security attacks than conventional wired and wireless networks. IDS attempts to detect and mitigate an attack after it is launched, and it is very important for the MANET security. It has three modules as depicted in Fig.1.

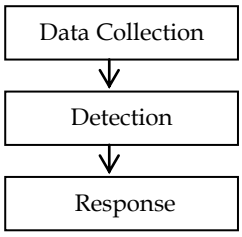


Fig.1. Modules

Data collection module collects the audit data from the node. Detection module checks whether there is any intrusion or not. If there is any intrusion, response module sends alert report to all the nodes. IDS can be categorized into two main parts: (i) architecture, which represents the operational structure of the IDS and (ii) detection engine, which is used to detect malicious behaviors [3].

The existing IDS architectures for MANETs fall under three basic categories [3] are (i) Stand-alone, (ii) Cooperative (iii) Hierarchical. The Stand-alone architecture uses an intrusion detection engine installed at each node utilizing only the node's local audit data. The Cooperative architectures include an intrusion detection engine installed in every node, which supervise local audit data and exchanges audit data and/or detection result with neighboring nodes in order to resolve inconclusive detections. The hierarchical architectures amount to a multilayer approach, by dividing the network into clusters. Special nodes are selected to act as cluster-heads and undertake various responsibilities and roles in intrusion detection that are usually different from those of those of the simple cluster members.

The intrusion detection engines are organized into three main categories[4]: (i) Signature based engines, which depends on the predefined set of patterns to identify attacks; (ii)Anomaly based engines, which depends on particular models of node behavior and declare nodes which deviate from these models as malicious and (iii) Specification based engines, which depends on a set of constraints such as either description of the correct operation of programs or protocols and supervise the execution of programs/protocols with respect to the constraints.

2. RELATED WORK

2.1 DoS attack

In this paper DoS attacks in MANET are focused. DoS attack is an attempt to make resources or services unavailable to their intended users. In MANETs, DoS attacks not only consume the scarce system resources like bandwidth, battery energy but also isolate legitimate users from the network [5]. Therefore, DoS attacks may affect the network connectivity seriously and degrade networking functions such as data and control message delivery. An attacker causes congestion in the network either by generating an extreme amount of traffic by itself or by having other nodes generate extreme amounts of traffic[6]. The wireless networks are difficult to prevent and protect against DoS attacks. They can cause a severe degradation of network performance in terms of the achieved throughput and latency. Defending against DoS attack in a MANET is challenging because the network topology is dynamic and nodes are selfish [7].

Adnan Nadeem et al.[8] proposed Hierarchical based IDS for DoS attack in MANET. They have used Adaptive Intrusion Detection and Prevention (AIDP) method to detect DoS attacks caused by Malicious RREQ Flooding in MANET. AIDP consists of Training module & Testing module. They divide the network into clusters then select the most capable nodes as Cluster Head(CH) and remaining nodes as Cluster nodes(CN). CH continuously collects information in the training module and produces an initial training profile (ITP). In the testing module the CH has the responsibility to identify the intruding nodes and isolate these nodes by informing all CNs.

Prajeet Sharma et al.[9] proposed a secure intrusion detection system against DoS attack in MANET. In their attack module they create one node as attacker node and set some parameter like scan port, scan time, infection rate, and infection parameter. The attacking node sends probing packet to all other neighbor node which is in radio range. If any node is a week node with nearby or in the radio range of the attacker node, then the attacking node receives probing packet and infects the nearby node and launches the DDoS (Distributed Denial of Service) attack and it may spread to next other node that causes the overall network, infected.

2.2 Chi-Square test

Chi-Square test has been applied as statistical technique on detection engine to detect the intruder in the following architectures: i)Stand-alone ii)Cooperative iii)Hierarchical iv)Zone based approach using mobile agent and listed out strength and weakness of each IDS architecture.

Chi-Square formula is

$$X^2 = \sum \frac{(\text{obs} - \text{exp})^2}{\text{exp}} \qquad (1)$$

where

obs = observed frequency
exp = expected frequency

2.3 Algorithm

The IDS algorithm has been implemented in three phases. They are: i) Analysis Phase ii) Detection Phase iii) Node isolation Phase. This uses Adhoc On Demand Vector (AODV) protocol. AODV uses the RREQ and RREP control packets for route discovery purpose. In analysis phase, RREQ received by all the nodes are observed and taken it as Observed frequency. Average of RREQ received by all the nodes was found and it has been taken as expected frequency. [8]

The algorithm has been applied in the different manner in MANET environment based on the architecture of IDS. If it is Standalone and Cooperative IDS, formula was applied in all the nodes. If it is hierarchical IDS, Cluster Head has the responsibility to monitor remaining Cluster nodes. So the formula was applied in Cluster Head node. If it is Zone based IDS, formula was applied in the Gateway nodes to monitor the activities of intra and inter zone nodes.

Analysis Phase

1. For all the nodes in the network
2. Monitor the number of RREQ received
3. Take it as observed frequency
4. Find the average of RREQ received by all the nodes
5. Take it as expected frequency

Detection Phase

1. Apply Chi-Square formula as in (1)
2. If Chi-computed value is > the Value that is obtained from degrees of freedom (Number of nodes-1) with 5% level of significance.
    a. Then reject the null Hypothesis(H0) and identify the intruder node
    b. Otherwise accept the null Hypothesis(H0)

Node Isolation Phase

1. If the node is identified as an intruder, response alarm will be sent to all the nodes.
2. The corresponding node will be isolated from the network.

Adnan Nadeem et al. [8] used Chi-square test with probability distribution to detect malicious node on hierarchical IDS in a MANET environment.

Rahul Rastogi et al.[10] built an IDS that can detect known and unknown attack automatically. Using a data mining framework, the IDS are trained by Chi-Square statistics to prevent the attacks and to make a Network Intrusion detection system (NIDS). This proposed model is used to detect anomaly-based network to prove the effectiveness of this statistical technique in detecting intrusions.

N.Ye et al.[11] presented an anomaly detection technique based on a chi-square statistic. This technique creates a profile of normal activities in an information system named as norm profile. It computes the departure of events in the recent past from the norm profile and detects a large departure as an anomaly-a likely intrusion. This technique differentiates normal events from intrusive events in an information system. The test results demonstrated the performance of this technique for intrusion detection based on a low false alarm rate and a high detection rate. Intrusive activities were detected at a very early stage.

2.4 Types of IDS

2.4.1 Stand-Alone Architecture

The stand-alone IDS architectures are based on a self-contained approach for detecting malicious actions at each node. In this architecture, an IDS is run on each node independently for deciding about the intrusions. Every decision made is based only on information collected at its

own node because there is no cooperation among nodes in the network. So no data is exchanged. No alert information is passed since the nodes in the same network do not know anything about the situation on the other nodes. Although this architecture is not effective due to its limitations, it may be suitable in a network where not all nodes are capable of running an IDS or have an IDS installed. This Architecture is also more suitable for the flat network infrastructure than for multi-layered network infrastructure. Since information on each individual node might not be enough to detect intrusions, this architecture has not been chosen in most of the IDS for MANETs [12].

V. G. Jecheva et al.[13] proposed an adaptive approach to anomaly based intrusion detection which is based on classification trees and string metrics. It detects an intrusion with high detection rate and low False Positive Rate.

2.4.2 Cooperative and Distributed architecture

The cooperative architecture includes an intrusion detection engine installed in each and every node. To determine inconclusive detections, it monitors local audit data and exchanges audit data and/or detection outcomes with neighboring nodes[3].

Since MANET is distributed and requires cooperation of other nodes in nature, ZhangandLee et al. [14] proposed the intrusion detection and response system in MANETs which is both distributed and cooperative depicted as shown in Fig.2. Each and every node participates in intrusion detection and response by running an IDS agent on them. It has the responsibility to detect and collect local data and events to identify promising intrusions, simultaneously initiate a response independently. When the evidence is inconclusive, neighboring IDS agents cooperatively participate in global intrusion detection actions. Similar to stand-alone IDS architecture, it is more suitable for flat network infrastructure, but not multi-layered one.

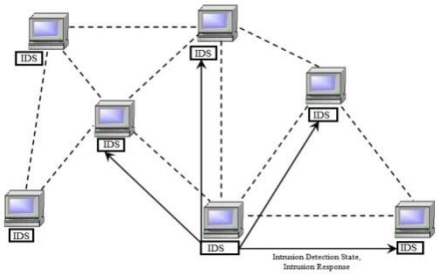


Fig.2. Cooperative IDS

Farhan et al. [15] presented the architecture and procedure of an ID technique in MANET. The proposed model is a distributed and cooperative architecture. The proposed ID technique combines the flexibility of anomaly detection with the accuracy of a signature-based detection method. To achieve efficient and effective intrusion detection they developed machine learning techniques.

S.S.Chopade et al.[16] presented an IDS to handle three types of internal attack such as resource consumption, route disruption and node isolation. The proposed work can be performed by modifying ad-hoc on demand distance vector (AODV) routing protocol. The intruder which has been detected in the detection phase should be isolated from the network in the recovery hase. Then the network is free from the intruder and provides the secure communication.

2.4.3 Hierarchical Architecture

In the hierarchical IDS architecture, the network nodes are divided into cluster-heads and cluster members. While the formers run a comprehensive engine that processes raw audit data from all the cluster members [3], cluster head runs a light weight local intrusion detection engine.

Adnan Nadeem et al.[8] proposed Hierarchical based IDS for DoS attack in MANET.

B. Pahlevanzadeh et al. [17] designed cluster-based distributed hierarchical intrusion detection system using mobile agents over Cluster-Based Routing Protocol (CBRP). It measures the efficiency of intrusion detection system in term of bandwidth utilization and energy consumption.

2.4.4 Zone Based Architecture

Sun et al. [18] have proposed an anomaly-based two-level non overlapping Zone-Based Intrusion Detection System (ZBIDS) by dividing the network into non overlapping zones 1 to 9 depicted in Fig.3. Nodes can be classified into two types: the intra zone node

and the inter zone node called gateway node. In zone 5, nodes b, c, h and k are inter zone nodes which have physical connections to nodes in other zones and nodes d, e, f and j are intra zone nodes.

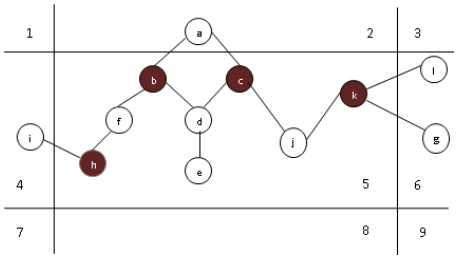
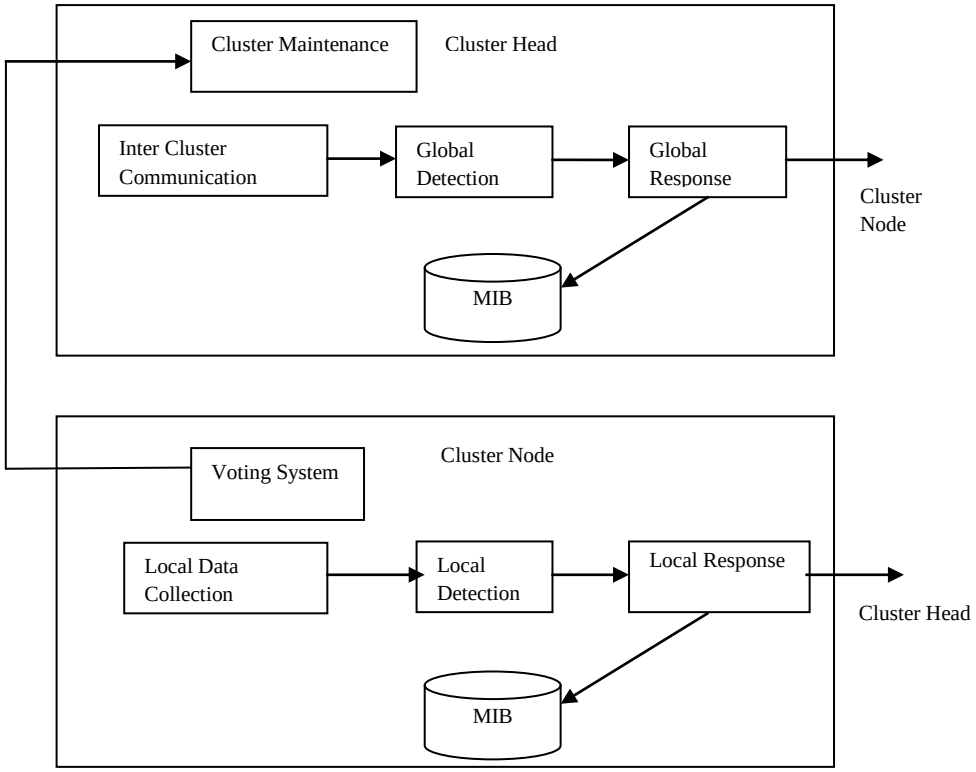


Fig.3.Zone based IDS

3. PROPOSED ARCHITECTURE



Farhan A.F et al. [19] proposed a hierarchical distributed model of multi-level intrusion detection system. It utilizes the intelligent, lightweight mobile agent and non overlapping zone framework. Some complicated attacks can be detected

The proposed architecture is the combination of hierarchical and Cooperative distributed architecture depicted in Fig.4. It consists of the following two modules: i) Cluster Head ii) Cluster Node module. Cluster Head module consist of Global Detection Agent, Global Response Agent, Inter cluster Communication Agent, Cluster Maintenance and MIB. Cluster Node Module consists of Local data collection

Agent , Local data detection Agent , Local Response Agent. Voting Agent and MIB. Each and every cluster node collects audit data and detects the intruder locally. If it identifies an intruder, it responds to the Cluster Head.

If the intruder is unidentifiable, it calls Cluster Head module. Then cluster head identifies an intruder globally. Then it sends an alert message to all the cluster nodes and isolates the malicious node from the network. Both Cluster Head and Cluster Node contain Management Information Base to store the attack patterns. Based on the patterns available in the MIB, Cluster Head and cluster node identifies an intruder. If an intruder is unknown, its pattern will be updated in MIB.

Local Data Collection Agent collects the local audit data on each node. Local Detection Agent detects an intruder locally. If any intruder is identified, Local Response Agent sends alert response locally to the cluster head. Global Detection Agent detects the intruder globally.

If any intruder is identified, Global Response Agent sends alert response globally to all the cluster nodes. Cluster Maintenance Agent is responsible for Cluster maintenance, Election supervision. Since MANET has the feature of mobility, Cluster Head may move from one cluster to another cluster and some new nodes may join in the current cluster which are monitored by this module.

Inter Cluster Communication Agent has the responsibility to interact with other clusters. If the Cluster Head Moves from current cluster to another cluster, immediately election should be conducted by Voting System Agent. Through this module, cluster nodes will poll their vote.

Cluster head and Cluster node identifies an intruder by checking the current pattern with existing pattern with existing pattern available in MIB (Management Information Base). All identified intrusion activities will be updated to MIB.

4. SIMULATION RESULTS

The performance of above IDS architectures have been simulated by NS-2 simulator [20]. Fig. 5(a) shows the Detection Rate Vs Node Speed. Fig. 5(b) shows the False Positive Rate Vs Node Speed. The following parameters are used throughout the experiments.

1. Routing protocol - (AODV), Mobility scenarios generated using a random waypoint model with 50 nodes
2. Moving in an area of 600m by 600m. The pause time between movements is 2 seconds Randomized TCP and UDP/CBR
3. We create 20 connections and the average traffic rate is 4 packets per second.

4. Maximum 2 to 3 intruders.

These parameters define a typical MANET scenario with modest traffic load and mobility

False Positive Rate (FPR) measures the number of misclassified positive instances inrelative to the total number of misclassified instances. Detection Rate (DR) is the proportion of correctly classified examples in relation to the total number of examples [19].

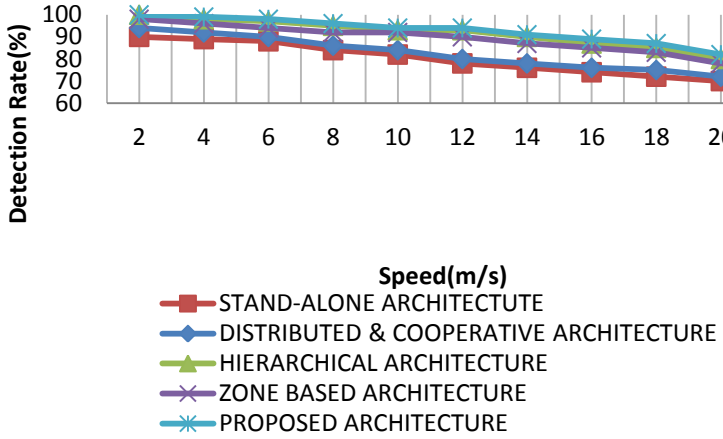


Fig.5 (a).Detection Rate Vs Node Speed

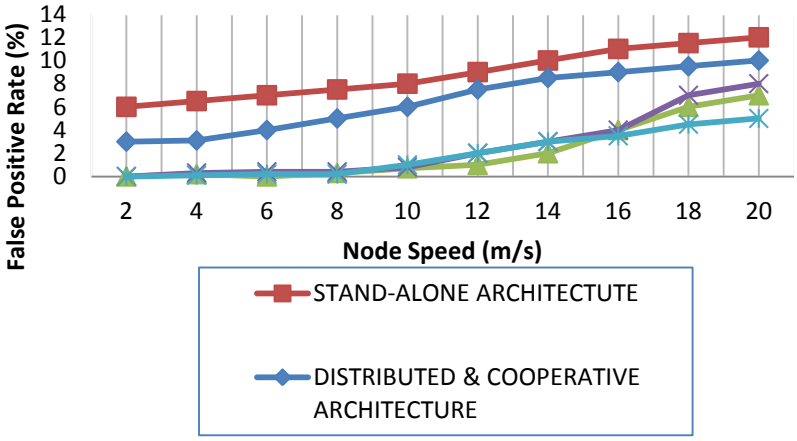


Fig.5(b).False Positive Rate Vs Node Speed

Table 1 shows the strengths and weaknesses of various IDS architecture

No.	Name of the Architecture	Strengths	Weaknesses
1.	Stand-alone IDS	1.Since it is the first architecture, it detects the intruders best on earlier days	1. There is no cooperation between the nodes. 2.It cannot detect Coordinated attacks
	Cooperative & Distributive IDS	1.Cooperation is achieved through theexchange of data and detection results with the neighboring nodes 2. Reduces communication overhead. 3. It is able to detect attacks at multiple Layers	1.Decison is made based on vote. 2.Since all nodes should have IDS agent on them, it increases network overhead. 3.Exchange of audit data increases communication over load. It may create some security risks.
3.	Hierarchical IDS	1. Nodes with the highest battery power may be elected as cluster heads. 2. Improves the efficiency based on resources. 3. Cluster Head has the responsibility to monitor the activities of cluster node.	1. Cluster Heads are overloaded. 2. Maintenance of cluster formation creates extra processing and communication overhead for cluster Head. 3.Sometimes Malicious node may be elected as Cluster Head.
4.	Zone based IDS	1.Detects the intrusions zone wise perfectly	1. Gateway nodes may be an intruder nodes
5.	Proposed IDS	1. Combines the feature of hierarchical and Cooperative IDS. 2. Cluster head is responsible for intra and inter cluster maintenance. 3.In case of failure of Cluster Head , immediately new cluster head will be elected	1. Malicious node may act as Cluster Head.

5. CONCLUSION

Security is the most important feature for deployment in MANETs. DoS attacks are more complex and serious problem in MANET, and as a result several approaches have been proposed to counter them. IDS as defense mechanism have been chosen. The results of them are listed. An architecture which is the combination of distributed and hierarchical IDS is proposed. The proposed architecture gives an improvement of Detection Rate and False Positive Rate over existing algorithms.

6. REFERENCES

[1] I.Chlamtac, M.Conti, N.Liu, Mobile ad hoc networking: imperatives and challenges, Adhoc networks, Vol. 1, no. 1, pp.13-64,2003.

[2] H.Yang, H.Luo, F.Ye, S.Lu, L.Zhang, Security in mobile adhoc networks: Challenges and solutions, IEEE wireless communications, Vol. 11, no. 1, pp.38-47, 2004.

[3] Christos Xenakis, Christoforos Panos, Ioannis Stavrakakis, A comparative evaluation of intrusion detection architectures for mobile ad hoc networks, Elsevier, pp.63-80, 2010.

[4] A.Mishra, K.Nadkarni, A.Patcha, Intrusion Detection in Wireless Ad hoc Networks, IEEE Wireless Communications, Vol. 11, Issue 1, PP. 48-60, 2004.

[5] Fei Xing Wenye Wang ,Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks, Military Communications Conference, 2006. MILCOM ,IEEE.

[6] International, 2001. Safdar Ali Soomro, Sajjad Ahmed Soomro, Abdul Ghafoor Memon, Abdul Baqi, Denial of Service Attacks in Wireless Ad hoc Networks, Journal of Information & Communication Technology, Vol. 4, 2010.

[7] XiaoxinWu, Beijing, DavidK.Y. Yau, Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering:A Game-theoretic Approach, ASIACCS'07, 2007.

[8] Adnan Nadeem, Michael Howarth, Adaptive Intrusion Detection & Prevention of Denial of Service attacks in MANETs, ACM, 2009.

[9] Prajeet Sharma, Niresh Sharma, Rajdeep Singh, A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network,

International Journal of Computer Applications, Volume 41, No.21, 2012.

[10] Rahul Rastogi, Zubair Khan, M. H. Khan, Network Anomalies Detection Using Statistical Technique: A Chi- Square approach, International Journal of Computer Science, Vol 9, 2012.

[11] N.Ye and Q.Chen, An Anomaly Detection Techniques based on a CHI-SQUARE Statistics for Detecting Intrusion into Information System, Quality and Reliability Engineering, 2001.

[12] T.Anantvalee, J.Wu, A survey on intrusion detection in mobile adhoc networks, Wireless/mobile network security, Springer, Chapter 7, pp.170-196,2006.

[13] V. G. Jecheva, E. P. Nikolova, An Adaptive Approach to Anomaly Intrusion Detection Based on Data Mining and String Metrics, International Review on Computers and Software, 2008

[14] Y.Zhang, W.Lee, Y.Huang, Intrusion Detection Techniques for Moble Wireless Networks, ACM WINET, Vol.9, No.5, 2003.

[15] Farhan A.F. , Zulkhairi D. , M.T. Hatim, Mobile Agent Intrusion Detection System For Mobile Ad Hoc Networks: A Non-overlapping Zone Approach , IEEE/IFIP, ICI 2008.

[16] S.S.Chopade, Prof.N.N.Mhala, A Co-Operative Intrusion Detection System in MobileAdHocNetwork, International Journal of Computer Applications,Volume 18, 2011.

[17] B. Pahlevanzadeh, S.A. Hosseini Seno, T.C. Wan, R. Budiarto, Mohammed M. Kadhum, A Cluster-Based Distributed Hierarchical IDS for MANETs

[18] B.Sun, K.Wu, U.W.Pooch, Alert Aggregation in Mobile AdHoc Networks, WiSe'03 and MobiCom'03, pp.69-78, 2003.

[19] Farhan Abdel-Fattah, Zulkhairi Md. Dahalin, Shaidah Jusoh, Distributed and Cooperative Hierarchical Intrusion Detection on MANETs, International Journal of Computer Applications, Volume 12, No.5, 2010.

[20] NS-2 Simulator. URL: http:// www.isi.edu / nsnam/ns.