International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008Certified Journal, Volume 4, Issue 5, May 2014)

Defend Mechanism Against Intruders In Multi-Hop Wireless Network

Ekta Upadhyay[1], Amit Mandloi[2]
[1,2]VITM, RGTU

***Abstract*—Mobile ad hoc networks are dynamic networks that can be formed without any fixed communication infrastructure. In addition to node mobility, ad-hoc network has limited resources such as bandwidth, battery power, and computational time. In such network the intermediate nodes serve as forwarder or relay nodes, which forward the packets. Security in such kind of network becomes a main concern to offers secure and reliable communication. The several kinds of attacks affect the network resources. On of them is internal attack which is performed by intruders. Intruders are internal node of the network which are compromised to influence network resources and degrades network performance. In this paper, several kinds of intrusions are described and detection approach for stand-alone intrusion also presented.**

***Keywords*—AODV, Intrusion Detection System,MANET, Routing, Attacks.**

I. INTRODUCTION

Network can be represented by the type of service it offers for communication of data. Out of these the majors are wired & wireless networks. As of now, the device portability is increasing day by day the hand held device mobility is also gaining popularity. The ad - hoc network is a wireless type of network. It uses open air communication channel and electromagnetic waves to send information between participants. Nodes in mobile ad-hoc network can communicate with every other node located within a specific distance, called the transmission range [1]. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. Mobile ad-hoc network resolve this problem by allowing intermediate nodes to relay data transmissions. When a node wants to communicate it sends a packet to another node that does not belong in its one-hop neighborhood then it has to rely to intermediate nodes to forward the packets to the final destination. Thus, effective routing protocols are required in order to optimize the route [2]. Security issues in wireless communication may also have a serious impact in other types of network architectures since several network architectures use wireless channels.

A. Routing in Ad-Hoc Network

Ad-hoc Network consists of a set of mobile hosts that carry out basic networking functions like packet relaying, routing, and service discovery without use of fixed infrastructure. Nodes of an ad hoc network relay on one another in forwarding a packet to its destination, due to the restricted range of each mobile host's wireless transmissions [3]. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to come into and leave the network as they want. Because of the limited transmitter range of the nodes, multiple hops are generally required to reach other nodes.

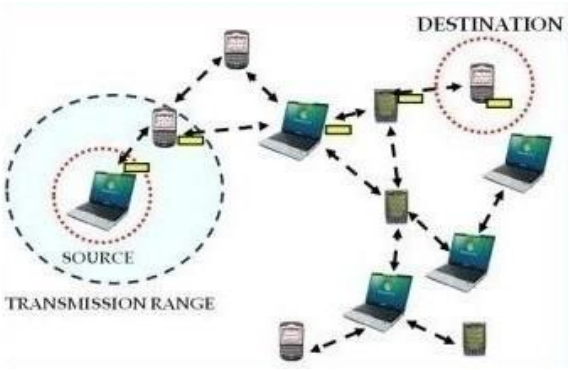

Figure1 Multi-hop Wireless Network

Ad-hoc Network consists of a set of mobile hosts that carry out basic networking functions like packet relaying, routing, and service discovery without use of fixed infrastructure. Nodes of an ad hoc network relay on one another in forwarding a packet to its destination, due to the restricted range of each mobile host's wireless transmissions [3]. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to come into and leave the network as they want. Because of the limited transmitter range of the nodes, multiple hops are generally required to reach other nodes.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008Certified Journal, Volume 4, Issue 5, May 2014)

B. Issues in MANET

There are several issues in MANETS which addresses the areas such as radio interference, routing protocols, power constraints, security, mobility management, bandwidth constraints, QOS, etc.; [5]. As of now some hot issues in MANETS can be related to the routing protocols, routing attacks, power and bandwidth constraints, and security issue, which have raised lot of interest in researchers. Even though in this paper we only focus on the routing attacks and security issue in MANETS.

The inherent features of mobile ad hoc networks make them more vulnerable to a wide variety of attacks by malicious nodes. Attacks can be categorized as passive and active attacks [6]. In active attacks, we mainly consider the internal attacks for network layer such as grey hole attack, worm-hole attack, black hole attack, message tampering, routing attacks. A malicious node drops packets or generates additional packets solely to disrupt the network performance and prevent other nodes from accessing any network services. These are employed using AODV (Ad hoc on demand distance vector protocol) routing strategy. This approach detects and prevents misbehaving nodes (malicious) capable of launching any of the network layer attacks. This work focus on improving the more secure mechanism to this forged message detection & valid packet dropping by malicious node detection. The identification of these malicious nodes requires some standard protocol parameters. Trust can be consider a well-known parameter for node behaviour whose value is continuously exchanged between all the adjacent neighbour nodes.

Security in MANET is the major concern, which deals with all the type of attacks & data packet security. Thus the node, which is involved in such type of security breaches, is called as malicious or misbehaving nodes & the mechanism used to prevent that comes under security system. These vulnerabilities can be prevented by various mechanisms like acknowledgement, monitoring nodes, behaviour detections, data dropping & modifications, delay reductions etc.

All the existing routing protocol assumes that the nodes within the range is behaving properly because they had not considered the mobility & network scenarios adoptions due to new nodes. Thus they are vulnerable to attacks launched by thesemisbehaving nodes & malfunctioning. However, there is not a deep study of the impact of such attacks on the performance of routing protocols through simulations. The existing static & dynamic routing protocols like ADOV, DSR, OLSR needs to be updated for providing better security against the issues.

The prime concern of this work is to suggest new updates for security is to demonstrate higher vulnerabilities detection rates with minimized performance issues.

II. Background

Intrusion is a kind of unwanted activity occurs in the network causes its degradation. Hence it has to be detected at early stagesof data transmission. This activity is going to be executed on malicious nodes in a range specific scenario. Multiple nodes can communicate simultaneously along with their routing topology updates at each node due to their mobility. This system is getting complex & weakness, which lead to most security problems. Intrusion detection can be used as another wall of defence to protect the network from such problems. If the intrusion is detected, a reaction can be initiated to prevent or minimize harm to the system. Intrusion detection can be classified based on analysing the historical data as either host-based or network-based. A network based IDS capture and analyses packets from network traffic while a host-based IDS uses operating system or application logs in its analysis.

A. IDS Types

Based on detection techniques, IDS can also be classified into three categories [7]. Anomaly detection systems create a comparable model in which the normal behaviour of users is kept in the system. The system compares the captured actual data with these existing profiles, and then identifies the deviation of behaviour from the baseline as a possible intrusion by informing system administrators or initializing a proper response. Another is misuse detection system. In this the system keeps patterns of known attacks and uses them to compare with the captured data. Matched pattern is treated as an intrusion like a threat detection system; it cannot detect new kinds of attacks. Last is a specification-based detection, which defines a set of constraints that describe the correct operation of a program or protocol. Then, it surveys the execution of the program with respect to the predefined constraints.

B. IDS Techniques in MANET

Network security involves all activities related to the security enhancement required for a network. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to beat such security breaches. Routing and security play a very important role for successful implementation of MANETs.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008Certified Journal, Volume 4, Issue 5, May 2014)

Among all of its available tools intrusion detection is one of the most promising ways of recognizing a possible attack before the system could bepenetrated. For analysing the security of wireless mobile ad-hoc networks, we need certain parameters [8]. The basic parameters for a secure system are: Authentication Confidentiality, Availability, Integrity, Non-repudiation & Scalability. Several techniques have been proposed to detect misbehaving nodes in a mobile ad hoc network. These techniques can be classified into three categories [9]:

1. *Reputation Based Technique):*It relies on building a reputation metric for each node according to its behavioral culture. An observing approach used by most systems in this category is called a watchdog. The watchdog was proposed to detect data packet noun forwarding by over-hearing the transmission of the next node.
2. *Credit Based Technique):*It is used to provide additional points of benefits for nodes to successfully perform networking functions. These values are trust index modifications methods by virtual (electron) currency or similar payment system. Nodes get paid for providing services to other nodes through these values. When they request other nodes to help them for packet forwarding, they use the identical payment system to pay for such services.
3. *Acknowledgement Based Technique):*It relies on the reception of an acknowledgment to verify that a packet has been forwarded & can be extended to multilevel acknowledgement.

C. Identified Protocols of Work

According to the behaviour of routing decisions, IDS can works in integration with various routing protocols such as proactive routing protocols and reactive routing protocols. Proactive routing called as a table driven routing in which the routes are discovered and updated periodically irrespective of data communication between nodes. Though routes are available instantly, the network overheads tend to be huge in high mobility and large networks. A popular pro-active routing protocols which can be used by IDS are Optimized Link State Routing (OLSR) routing and Destination Sequence Distance Vector routing (DSDV). Reactive routing on the other hand discovers routes only when a node requires a communication channel to send data for a particular receiver. Hence reactive routing is also called as on demand routing protocols. Popular reactive routing protocols include Ad hoc-On-demand Distance Vector (AODV) routing protocol and Dynamic Source Routing (DSR) [10].

D. IDS Architecture

Over the last few years the various architectures of MANET are being proposed to solve the issues related to intrusion detection systems. While considering the various types of network scenario such as in flat network infrastructures, all nodes are taken as equal. In multilayer infrastructures, all nodes are different. Nodes may be grouped in clusters having similar characteristics, with a cluster-head node for each cluster. For communication in intra-cluster, nodes are in direct contact with cluster head. Nodes communication between inter-clusters is performed through each cluster-head nodes. This infrastructure is suitable for applications satisfying military needs. According to [11] this architecture is broadly classified into four major classes. These are:

1. *Stand Alone IDSS):*In this every node is having dedicated IDS for itself & is responsible for each decision, which a node can take, based oncollecting data. It has no interaction between network nodes and therefore no information is interchanged like position of other nodes, alert information etc. Even though, due to its limitations, they are not effective, but they can be suitable for networks where nodes are not capable of executing an IDS or where an IDS has been installed. The node information & IDS selection criteria is not that effective in this so it is not used to widely accept the flat network.
2. *Distributed and Cooperative IDSS):*The above issue of stand-alone IDS is resolved when we can be able to share the execution information about IDS & its result among various nodes in its range. It can be done via using the concept of distributed and dependent nodes cooperation. Each node collaborates in intrusion detection and an action is performed by an IDS agent on it. Each IDS agent is accountable for detection, data collection and local events in order to detect intrusions and generate an individualistic response. Even though neighboring IDS agents cooperate with each other whenthere is not any convincing evidence in global intrusion detection.
3. *Hierarchical IDSS):*This IDS architecture is a well formulated distributed & cooperative mechanism used for multilayer infrastructure based clustered environment. It has individual cluster heads works as control points like network device such as a switch, router or gateway. This cluster head has all the functionalities to identify those malicious behaviors. They can be able to monitor network traffic and packets, which help in detection of unwanted activities.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008Certified Journal, Volume 4, Issue 5, May 2014)

4. *Mobile Agent for IDSS):*To this type of IDS the malicious behavior identification or outlier detection can be given to mobile nodes called as mobile agent. Due to its movable nature, each mobile agent is considered for performing just one special task and then one or more mobile agents are distributed amongst network nodes. It makes IDS distributed in nature Due to that some responsibilities are not given to every node, and so it helps in reducing the energy consumption. It also provides for fault tolerance in such a way that if the network is segmented or some of the agents break down, they can still continue to function. It can also be work for the larger mobile environment.

III. LITERATURESURVEY

During the last few years various researchers have focused there work nearly to security from an intrusion processes. They had developed various intrusion detection systems to overcome the vulnerabilities related to intruder's process. Some of them studied here, related to this work is given as:

Farhan et. al. in 2008 proposes a novel intrusion detection method by combining two anomaly methods Conformal Predictor k-nearest neighbour and Distance based Outlier Detection (CPDOD) algorithm [12]. A sequence of experimental results shows that the proposed method can effectively detect anomalies with high detection rate, low false positive rate and achieve higher detection accuracy. The proposed approaches describe a combined model that uses two different measures (nonconformity metric measures and Outlier Factor LDOF metric) to improve its detection proficiency. Nonconformity metric measures whether the unknown instance is more similar to known normal instances or abnormal instances. Continuing the above research concern Vinay et. al. gives an study on various architecture of IDS in the manuscript [13] to achieve the reliable and confidential transmission over MANET which follows some techniques such as, Confident, Watch Dog and CORE.

In this paper [14], Devi et. al. have studied the impact of DDoSattacks over MANET. The work also gives a design-based scheme to overcome the DDoS attack in a Mobile Ad-hoc Network. It uses cluster analysis along with XOR marking to detect and prevent the effects of DDoS attacks in the network. The performance analysis was made for the packet acceptance rate and to find the attack detection. From the experimental results obtained, it is justified that the proposed scheme is more efficient to overcome the DDoS attacks in a ad-hoc network.

Some of the researchers also focused their concern in analyzing the data for intruder's packet. For this they used various mining approaches. Among them most of it uses classification techniques. In order to do so Aikaterini et. al. in [15] evaluates five supervised classification algorithms for intrusion detection on a number of metrics. The work measures the performance of these classification algorithms on various datasets, which includes varied traffic conditions and mobility patterns for multiple attacks. The paper investigates following concerns:-

- How classification performance depends on the problem cost matrix.
- How the use of uniform versus weighted cost matrices affects classifier performance.
- Which techniques are used for tuning classifiers when unknown attack subtypes are expected during testing?

Consequently, they tried to develop a sequential cross-validation procedure so that not all types of attacks will necessarily be present over all folds, in the hope that this would make the tuning of classifiers more robust. The results of proposed area indicates that weighted cost matrices can be used effectively with most statistical classifiers and that sequential cross-validation can have a small, but notable effect for certain types of classifiers.

In 2010 the paper [16] by Rakesh et. al. proposes a novel cross layer intrusion detection architecture to discover the malicious nodes. The work also gives a study on specific type of attack which can occurs likewise always in case of intrusion like DoS attacks. By identifying these attacks & exploiting the information available across different layers for those, the work will improve the accuracy of detection. It uses cooperative anomaly intrusion detection with data mining technique to enhance the proposed architecture. The simulation of the proposed architecture is performed in OPNET simulator and gives better results. Some of the improvement suggestions in the IDS architecture is given by [17] & [18] through their reputation value using adaptive decision boundary. The work depends on current strength of nodes & identifying the selfish behavior through reputation calculation and classification. It also saves energy of other nodes as energy is a major challenge of MANET.

In 2013, Vigneshwari et. al. gives an alternate way of IDS using data classification. The paper proposes an approach of trust model design that provides nodes with a mechanism to evaluate the trust of its neighbors. In this a node assigns a so-called trust level for each of its neighbor, which represents how reliable each neighbor is. It is based on previous successful transmission of data.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008Certified Journal, Volume 4, Issue 5, May 2014)

It observes node's mobility, number of neighbors each node has, number of packets generated and forwarded by the neighboringnodes [19], finding the malicious node and calculate these parameters to determine which nodes are misbehaving in the network and performance is improved by avoiding requesting and verifying certificates at every routing step. At the initial level of research the approach seems to provide better result in near future.

Various other approaches is proposed in last few years based on existing mechanism like watchdog in [20, 21]. As the main advantage of it is that the watchdog only needs local information and, therefore, it becomes quite difficult for it to be badly influenced by another node.

But it has two disadvantages

- Watchdog is not appropriate for cooperative attacks
- It is not so accurate when nodes mobility increased.

Tushar et. al & Hijung et. al. also proposes an improvement in this mechanism which can be used in MANET. The watchdog is a basic approach for several different IDS, doing an extra effort for improving it becomes a necessity. The proposed improvements can cope up well with the watchdog weaknesses based on kalman filters. Another improvement of the approach is avoidance of collaborative black-hole attack. A secure exchange of information among nodes allows determining whether if a node is acting as an accomplice, and also marks it as being malicious.

Redesigning of intrusion detection architecture can be accomplished by using the timestamp based trust models as suggested in [22]. In this, the participating nodes are permissible to listen the transmission of the neighboring nodes in monitoring mode. At this point within a certain timeframe the message is not relayed, and then the node is recommended to be tagged as a misbehaving node. Depending on the behavior the tagged packet can be separated from untagged packets & node can be easily categorized. A simple & effective simulation is shown in that.

In 2013 Muhammad et. al. in [23] surveyed the attacks that target ad hoc routing protocols focusing on the OLSR protocol. The work created a unique description model of attack categorization on the basis of which correct IDS can be applied. Approach tries to develop a new lightweight IDS based on signature verifications through a log based IDAR. It distinguishes itself by analyzing the logs generated by a routing protocol and extracts intrusion evidences so as to compare these latter against predefined intrusion signatures.

The work further categorizes the evidence into four groups according to their degree of maliciousness. At the initial level of research & consecutive simulations study, approach is providing effective results.

IV. Proposed Approach

In the ad-hoc network, intruders are compromised or cooperated node, which influence network resources, degrade network performance and drain battery life of genuine nodes. To detect intruders, an approach advised which maintain record of data packet and RREQ and RREP packet at specific node and Xoring of value of forward and receive of packets and analysis the behavior. If the value of Xoring is 0 then node is recognized as intruders otherwise node is normal.

A. Algorithm

```
Algorithm Int_Node (node,n)
{
DECLARE F_packet, R_packet

// To keep all possible record for each node in different cases for each neighbor node of selected node
Case1:
        F_packet=0 and R_packet=0
Case2:
    F_packet=1 and R_packet=0
Case3:
    F_packet=0 and R_packet=1
Case4:
    F_packet=1 and R_packet=1
//To check the value of XORing of F_packet and R_packet to take decisions for intrudes
If (F_packet XOR R_packet==0) then
DISPLAY "Node is normal"
ELSE
DISPLAY "Node is intruders"
End If
Exit
```

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459,ISO 9001:2008Certified Journal, Volume 4, Issue 5, May 2014)

B. Flow Chart

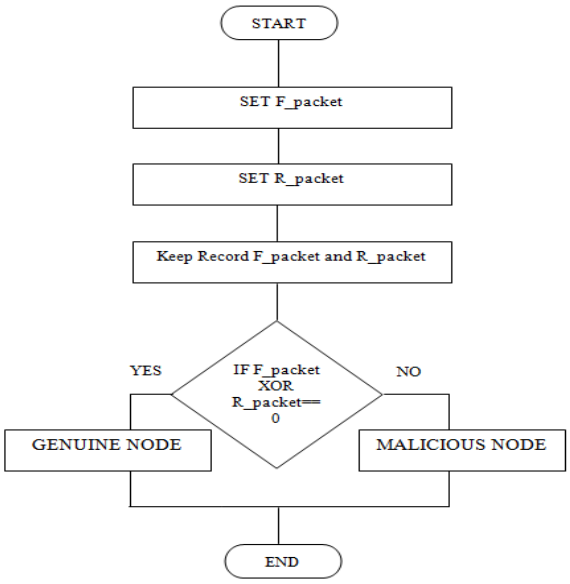

Figure2 Work Flow of Proposed Approach

V. CONCLUSION

In mobile ad hoc networks, protecting the network resources from attacks is an important research topic in wireless security. The proposed approach describes a robust and security service scheme for network-layer security solution in ad hoc networks, which preserve both, routing and packet forwarding functionalities without the context of any data forwarding protocol. This approach solves the issue in an efficient manner. The overall idea of this approach is to detect intruder launching attacks and misbehaving links to prevent them from communication network. It is a robust and a very simple idea, which can be implementedand tested in future for more number of attacks, by increasing the number of nodes in the network and routing protocols.

REFERENCES

[1] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", in Proceedings of MOBICOMM Boston USA, ACM Special Issues, DOI: 1581971136, 2000.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] Yongguang Zhang and Wenke Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom'2000), ACM Special Issues, 2002.

[3] Yian Huang and Wenke Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", in College of Computing Georgia Institute of Technology, USA.

[4] Yih-Chun Hu and Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security & Privacy, ISSN: 1540-7993/04/, 2004.

[5] Levente Butt and Jean-Pierre Hubaux, "Report on a Working Session on Security in Wireless Ad Hoc Networks", in Mobile Computing and Communications Review, NCCR-MICS grant number 5005-67322, Volume 6, Number 4, 2005.

[6] Chin-Yang Tseng, Poornima Balasubramanyam and Calvin Ko, "A Specification-based Intrusion Detection System for AODV", in Computer Security Laboratory, University of California, Davis.

[7] Umesh Prasad Rout, "A Study of Intrusion Detection Systems in MANETs", in International Journal of Research in Computer and Communication Technology, ISSN(Online) 2278-5841, Vol. 2, Issue 2, Feb-2013.

[8] S.Sasikala and M.Vallinayagam, "Secured Intrusion Detection System in Mobile Ad Hoc Network using RAODV ", in Proceedings published in International Journal of Computer Applications (IJCA), ISSN: 0975 – 8887, ICRTCT-2013.

[9] Sagar Pandiya, Rakesh Pandit and Sachin Patel, "Survey of Innovated Techniques to Detect Selfish Nodes in MANET", in International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), ISSN 2250-1568, Vol. 3, Issue 1, Mar 2013, 221-230.

[10] S. P. Manikandan and Dr. R. Manimegalai, "Evaluation of Intrusion Detection Algorithms for Interoperability Gateways in Ad Hoc Networks", in International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol. 3 No. 9 September 2011.

[11] Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi, "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes", in World Academy of Science, Engineering and Technology, 2008.

[12] Farhan Abdel-Fattah, Zulkhairi Md. Dahalin and Shaidah Jusoh, "Dynamic Intrusion Detection Method for Mobile Ad Hoc Network Using CPDOD Algorithm", in IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.

[13] Vinay P.Virada, "Intrusion Detection System (IDS) for Secure MANETs: A Study", in International Journal of Computational Engineering Research (IJCER), ISSN: 2250-3005, Vol. 2 Issue. 6, October 2012.

[14] Aikaterini Mitrokotsa and Christos Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", in Science Direct Elsevier Publication, Journal of Ad-Hoc Networks, ISSN: 1570-8705, available at http://dx.doi.org/10.1016/j.adhoc.2012.05.006, 2012.

[15] Rakesh Shrestha, Kyong-Heon Han, Dong-You Choi and Seung-Jo Han, "A Novel Cross Layer Intrusion Detection System in MANET", in IEEE International Conference on Advanced Information Networking and Applications, ISSN 1550-445X/10, DOI 10.1109/AINA.2010.52, 2010.

[16] Farzneh Pakzad, Marjan Kuchaki Rafsanjani and Arsham Borumand Saeid, "The Improvement Steps of Intrusion Detection System Architectures of MANET", in IJMAS, ISSN: 0973-7545, Vol. 22, Issue S11, 2011.

[17] Amir Khusru Akhtar and G. Sahoo, "Classification of Selfish and Regular Nodes Based on Reputation Values in MANET Using Adaptive Decision Boundary", in Science Research Journal of Communications and Network, ISSN: 0185-0191, doi:10.4236/cn.2013.53021, May 2013.

[18] P.Vigneshwari, R.Anusha, D.Preethi , R.Jayashree and V.Nandhini, "Comparative Analysis of AODV and Trusted AODV (TAODV) in MANET", in International Journal of Advanced Information Science and Technology (IJAIST), ISSN: 2319:2682, Vol.10, No.10, February 2013.

[19] Tushar Sharma, Mayank Tiwari, Prateek kumar Sharma, Manish Swaroop and Pankaj Sharma, "An Improved Watchdog Intrusion Detection Systems In Manet", in International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 3, March-2013.

[20] Huijun Chang, Hong Shan and Tao Ma, "Segmentation, Clustering and Timing Relationship Analysis of MANET Traffic Flow", in TELKOMNIKA, ISSN: 2087-278X, Vol. 11, No. 8, August 2013, pp. 4817~4823.

[21] Charlie Obimbo and Liliana Maria Arboleda Cobo, "An Intrusion Detection System for MANET", Communications of Information Science and Management Engineering (CISME), Vol.2 No.3, 2012. pp.1-5

[22] Yi Li and June Wei, "Guidelines on Selecting Intrusion Detection Methods in MANET", in Proc. of ISECON (EDSIG), Vol.21, (Newport): §3233 (refereed), 2004.

[23] Mouhannad Alattar, Françoise Sailhan and Julien Bourgeois, "Lightweight Intrusion Detection: Modeling and Detecting Intrusions Dedicated to OLSR Protocol", in International Journal of Distributed Sensor Networks Volume 2013, Article ID 521497, 20 pages at http://dx.doi.org/10.1155/2013/521497.