A Novel Feature based Unified Node Data Analysis (FBU-NDA) based IDS using AODV in MANET

Trupti Agrawal
PG Scholar, Computer Science & Engineering,
Oriental University, Indore, India

Swati Tiwari
Asst. Professor, Computer Science & Engineering,
Oriental University, Indore, India

ABSTRACT
MANET is a type of wireless network, which works on radio frequencies and holds short range communication. As it is temporary in nature and is having movable devices for communication which makes such network as infrastructure less. In such network variable conditions of routing will face several issues which degrade its performance. Out of these securities 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 intrusion detection system. These intrusions can be prevented by various mechanisms like acknowledgement, monitoring nodes, behavior 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 newly identified nodes. Our prime concern by proposing new updates for security is to demonstrate higher intrusion detection rates with minimized performance issues. This work proposes a new improved Feature Based Unified Node Data Analysis (FBU-NDA) Based IDS through AACK for AODV protocol. This quantity of response can be taken as major consideration for identification of intruder's node.

Keywords
MANET (Mobile Ad-Hoc Network); AODV (Ad-Hoc on Demand Distance Vector), Feature Based Unified Node Data Analysis (FBU-NDA); IDS (Intrusion Detection System);

1. INTRODUCTION
Ad-Hoc network is a wireless network which works without any infrastructural requirements for transmission. It works in a small distance communication area and performs routing in absence of any router. This functionality is embedded to its individual participating nodes like any mobile devices, PDA or laptops. As, its working range is very less thus its protocol designing is also of different type which follows lightweight approaches. In this nodes are always in mobility with respect to their positions and hence topology is also dynamic, but its applicability areas are very vast. As the wireless medium is gaining popularity such ad hoc network use is also serving as a best option for small communications. MANET, WSN, ZigBee, Cognitive and VANET are the well known example of ad-hoc networks. Among them MANET is a very rapidly growing type of network because of its dynamic nature of communication. It can be of single hop & can be extended to multi hop. It is flexible in nature and hence the application area is also very large such as military, transport, aviation, commercial etc. 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]. MANET solves this problem by allowing intermediate parties 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, efficient routing protocols are required in order to optimize the communication paths [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.

The default nature of MANET and its wide variety of devices move-in and out of very small range causes frequent modification in topologies which provides the space for attacker to disrupt networks normal working. Thus it raises the security risk associated with transmission. It always needs some new approaches hitting to market for resolving those security breaches for effective and continuous working. As the security mechanism becomes stronger, the type of attacks and their vulnerability is varying very frequently causes failure of existing detection mechanisms. Deviation of working or behavior from actual to some uncertain conditions called as maliciousness. It affects both nodes and routing because of unavailability of restrictions. Nodes intentionally drop the working of network called as intruders. In order to prevent deceptive outside node entering the network, some sure authentication & encryption methods can be used. Most of the attacks in mobile environments focus on routing protocols. These protocols were firstly designed to be efficient without taking into account the security issues. They usually need the cooperation between the participants and assume confidence between them. Nevertheless, a malicious node may modify its supposed benign functionality disturbing the overall behavior of the protocol. This malicious behavior of node needs to be identified at the early stages of communication & comes under the intrusion detection. It can be defined as a process of monitoring activities in a system, which can be a computer or network system or a user. An Intrusion Detection System (IDS) collects activity information of the various nodes in its range and then analyses it to determine whether there are any activities that violate the security rules. Once an ID determines that an unusual activity or an activity that is known to be an attack occurs, then the system generates an alarm to alert the security administrator [3]. In addition ID Scan also initiates a proper response solution of removing such malicious activities.

2. BACKGROUND

Intrusion is an unauthorized activity operating in network causes drops in its performance. It affects the actual working of devices and hosts thus needs to be detected in early stages of communications. The node behaving as such unauthorized called as malicious node. In MANET nodes are communicating in absence of any fixed infrastructure and hence the protocol working on each is also lightweight. These protocols are not able to analyse the maliciously behaving nodes and intrusion activity performs which leads to data loss. Even the topology of network is also very abruptly changes because of heavy motions or mobility of nodes and causes normal characteristics of network to be changed. Such frequent changes raises complexity and weakness of the system and vulnerability to attacks like intrusions is increased. Intrusion detection system is the mechanism used to detect such unwanted access and changes to the network. If the intrusion is detected, a response 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.

2.1 IDS Types

Based on detection techniques, IDS can also be classified into three categories [3]. Anomaly detection systems create a comparable model in which the normal behavior of users is kept in the system. The system compares the captured actual data with these existing profiles, and then identifies the deviation of behavior from the baseline as a possible intrusion by informing system administrators or initializing a proper response. Another is misuse detection systems. In this the system keeps patterns of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus 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 monitors the execution of the program with respect to the defined constraints.

2.2 IDS Techniques in MANET

Routing and security play a very important role for successful implementation of MANETs. Network security sustains all actions related to the security improvement required for a network. A valuable network security strategy requires identifying threats and then applying the most proficient set of tools to beat such issues. Among all of its available tools intrusion detection is one of the most capable ways of recognizing a possible attack before the system could be penetrated. For analysing the security of wireless mobile ad-hoc networks, we need certain parameters [4]. The basic parameters for a secure system are: Availability, Confidentiality, Authentication, Integrity, No 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 [5]:

2.2.1 Reputation-Based Technique:

It relies on building a reputation metric for each node according to its behavioral pattern. A monitoring method 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.

2.2.2 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 same payment system to pay for such services.

2.2.3 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.

According to the behavior 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 destination. 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) [6] & [7]. Other approaches will be covered in next section which includes study about several approaches after which a comparison can be made for further improvements.

3. LITERATURESURVEY

During the last few years various approaches has been suggested for timely and effective detection of intrusions activities. As the intrusions process differentiation form the normal can be measured by analyzing the behavior at both the cases. Thus the suggested mechanism mainly involves data measurements and verifications. Few of them are given here as follows:

In 2008, a novel approach for intrusion detection is suggested based on two data mining algorithms conformal predictor k-nearest neighbor and distance based outlier detection as given in [8]. The mechanism improves the detection accuracy through metrics based approach applied by using above two algorithms. They measure the unknown instances occurring in the system and let the values compared in both the cases like normal and abnormal. At the experimental evaluations the approach is giving effective results. But to calculate conformity requires complete data which is not available always in mobility based networks. Hence some survey based modification is been suggested by [9]. Mainly this paper gives reliable and confidential transmission strategies in MANET. The paper also gives a comparison of existing approach like Watchdog, Confidant and core algorithms.

Carrying forward the above research paper [10] had presented a study on impact of Distributed Denial of Service (DDoS) attacks over MANET. It also gives a design based scheme to defeat the DDoS attack using cluster analysis along with XOR marking. 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 an ad-hoc network. Several researchers also focused their concern on analyzing the data for intruder's packet. For this they used various mining approaches like classification, clustering etc. Another approach based on mining is supervised classification algorithms for intrusion detection which evaluates results on various metrics as given by [11]. The work also measures the performance of these classification algorithms on various datasets which includes varied traffic conditions and mobility patterns for multiple attacks. The technique suggested by author is 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 across 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 significant effect for certain types of classifiers.

In 2010 the paper [12] 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 [13] & [14] through their reputation value using adaptive decision boundary. The work depends on current strength of nodes & identifying the selfish behaviour through reputation calculation and classification. It also saves energy of other nodes as energy is a major challenge of MANET.

In 2013, some extensions to classification based approach are proposed through trust model design. It provides nodes with a mechanism to evaluate the trust of its neighbors. Here each 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. . It observes node's mobility, number of neighbors each node has, number of packets generated and forwarded by the neighboring nodes [15], 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. Watchdog and Path-rater are some mechanism which is suggested by [16] and [17] which 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 vulnerable to cooperative attacks and it is not so accurate when there is sudden increased mobility. Some of the given improvements can cope up well with the watchdog weaknesses based on Kalman filters. 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 [18]. 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.

While selecting the IDS for specific applications, the criterion needs to be properly understood. Some guideline is suggested in [19]. This guideline is generated after analyzing various systems under different conditions & their evaluations is measured in terms of parameters. It is shown in [20]

In 2013 [21] & [22] 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. At the initial level of research & consecutive simulations study, approach is providing effective results.

4. PROBLEM STATEMENT

Condition of MANET frequently changes with its dynamic topology modifications by nodes mobility and hence the generation data and pattern analysis for intrusion identification becomes more complicated. For accurate intrusion and recognition some timely analysis is required on generated data for abnormality behavior detections. Also the attacks vulnerability and its types also changes with environmental conditions thus mechanism needs to be of dynamic behavior which is capable of taking the decision according to the situations. The type of attack behaves by manipulating routing information, either externally by passing false routing messages or internally by maliciously changing route cache information. Existing work analyses only few parameters for intrusions identification which needs to be modified. Some of the identified parameters are sent packets; receive packets, response count, PDR, throughput, change route entries, changed number of hops and number of neighbors. On these parameters existing work is not giving accurate analysis so as the intrusions recognition is not properly measured. Some of the identified issues which remain unsolved in existing mechanism are taken as problem identified for this work. These are:

Problem 1: In the existing mechanism cross validations of behavior of each node is not yet performed thus their parameter selection is also weak which not covers each aspects of intruder's measurement.

Problem 2: Partial drops and corruption in packets is also not given by any approach which leads us incorrect detections which later on affects the transmission by malicious node behaving as intruders.

Problem 3: Denial of service and distributed denial of service is only give by rejected request number which might be happens due to dropped connection and in such cases actual node might consider as intruders and hence the detection mechanism fails.

Problem 4: False route updates and traffic pattern distortion is unavailable with existing approaches.

Thus without the above intruders criteria the mechanism is not able to correctly identify the malicious behavior. Consequently, researchers have been working recently on designing new IDSs for MANETs or changing the current IDSs to be applicable to MANETs. There are new issues which should be taken into account when a new IDS is being designed for MANETs. The open medium and broad distribution of nodes make ad-hoc network vulnerable to intruders. Due to the node's lack of physical security, malicious attackers can easily capture and compromise nodes to achieve attacks. Hence the algorithms need to be updated for providing effective detection. Thus this work gives a detailed measurements based on unified detection approach for effective detection and removal.

5. PROPOSED FBU-NDA APPROACH

An intrusion is a kind of vulnerability which might affect the actual working of the system. As seen by various existing approaches, security breaches can be avoided by making timely detection and removal of unidentified intruders system. Identification of such process can be applied by using various methods suggested over the last few years for access control and authentications for unauthorized users or nodes. This work gives a novel Feature Based Unified Node Data Analysis (FBU-NDA) approach for effective and timely detection and removal of intrusions. The approach is capable of identifying the timely attacks and planned system attacks by humans malicious activities. Primarily, it works for mobile ad-hoc networks which are having dynamically changing topologies due to nodes mobility.

In such network there are very abrupt changes due to large scale motion of nodes and hence the connecting conditions and authorization process is very tedious. The suggested approach keeps its intensions on detection of malicious misbehaviours by measuring the triggering conditions of collisions, partial dropping and false misbehaviors.

The proposed scheme of FBU-NDA (Feature Based Unified Node Data Analysis) is designed to resolve the weakness of existing Watchdog and Pathrater approaches. Both the approaches mislead the detection because they are not capable to detect the false misbehaviour reports. In this the malicious nodes falsify the innocent node by its presence and later on disrupt the communication. The drops in data packets can be notified to destination nodes and the source node after which the drops path can be removed from their routing table entry. If there is no other that exists, the source node starts a routing request to find another route using AODV protocol. Due to the nature of ad-hoc networks, it is common to find out multiple routes between two nodes. The FBU-NDA approach work in three phases given as:

5.1 Feature Based Data Analysis

In this phase the data of previous communications is taken from different hosts and routes. This generated data contains the records for each node participating in the transfer. These generated data is analyzed to identify the useful patterns having malicious behaving indications based on their features. Thus features are extracted in this by a detector unit which contains the nodes information their topologies, routes, etc.

5.2 Intrusion Identification

After the feature based patterns is detected FBU-NDA analyzes them for behavior detection of each node. CNC work as a protocol stack and have various parameters for this malicious behavior identification. It includes their counts, neighbor's information, and packets transmission information like sent and receives packets along with acknowledgement counts. These fields are stored in the data store for monitoring purpose from which decision are taken respectively for intruder's behavior. From this stored information false behavior, collision and partial drops are measured for each nodes and routes. It gives detailed analysis of packet & behavior monitoring of each node within a specific range.

5.3 Removal and Updations

This phase is a conditional verification of stored data in which finally the throughputs and PDR is plotted. It gives the response counts and checks the condition for PDR and Throughput should be less than a defined threshold limit. If the threshold values and total measured parameters are going down from the actual value of normal nodes then a response is forwarded to each participating node so as the intruders nodes entry can be deleted from routing tables.

Pseudo code:

```
Intrusion Monitor ( )
 {
  Feature Based Unified Node Data Analysis ( )
  Nodes Count ();// Total Number of Packets Sent & Received
  Neighbor Count (); //Listen Neighbors Transmission
  Report Count (); //After fixed Period of Time Nodes Give report to Node
  Calculate PDR, Throughput for Each Node
  If (PDR, Throughput < Threshold)
  Intrusion detected (Categorized According to Threshold Attack Packets)
  If the node is moving out of Node Range
  Then Packet Dropping Attack Can Occur
Generate Local or Global Response to Modified IDS (Return);
 }
```

The intruder's behavior is abnormal from the original behavior and hence the detection is measured by the changes occurring in the network. The partial drops measurement is a complicated task because in this a ratio of data or other packets is dropped. Thus a checksum can be used for full packets transmissions. The approach depends upon the pattern of analyzed behaviors and comparison takes place with normal ones.

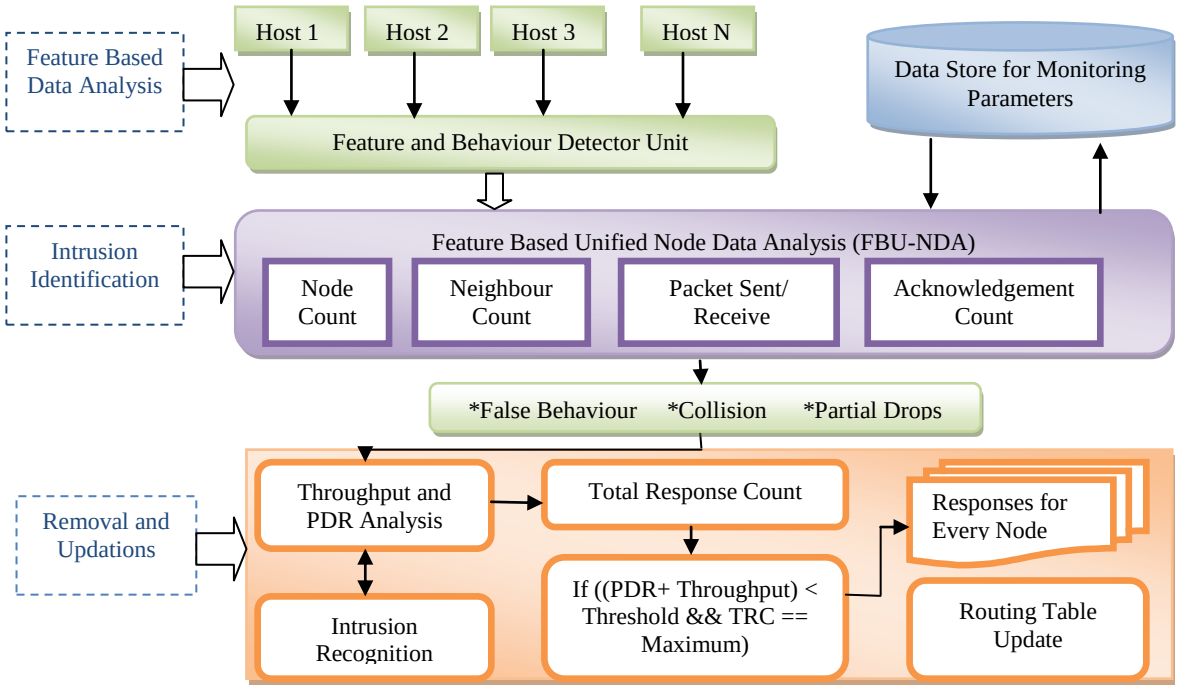

FIGURE 1: FEATURE BASED UNIFIED NODE DATA ANALYSIS (FBU-NDA) BASED IDS

6. EXPECTED OUTCOMES

As the suggested approach seems to solve the existing issues of IDS in MANET and leads to effective detection and removal of intruder's activity. In order to measure and compare the performances of the proposed FBU-NDA scheme, the work continue to adopt the two performance metrics, First is Packet delivery ratio (PDR) which defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. Second is Routing overhead (RO) which defines the ratio of the amount of routing-related transmissions such as RREQ, RREP, ACK, 2ACK, S-ACK etc. The proposed mechanism can be able to identify the attacks based on their types. This can be prevented before any damage or packet drops. In order to evaluate the effectiveness of the employed algorithms for the problem of intrusion detection following outcomes seems to be measured:

(i) Mobility based intrusion detection which overcomes the issues of ambiguous collision.
(ii) False misbehavior detection by analyzing the identity and behavior of nodes.
(iii) Partial drops are detected through a central monitoring node.
(iv) Secure transmission and cooperative attack detection.
(v) Packet dropping and flooding preemptions removal.
(vi) Forging attack is timely measured with data analysis module through collector and transmission data storage.

7. CONCLUSION

Intruders can easily compromise ad-hoc networks by inserting malicious or non-cooperative nodes into the network. Furthermore, because of network distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in an ad - hoc network. In such scenario, it is important to develop an intrusion-detection system (IDS) due to the limitations of most MANET routing protocols, nodes in networks assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. In this paper, the work studied various existing mechanism to make some preventions regarding these intrusions. But they have some negatives also like timely analysis of misbehaving nodes, false identification, collision detection, central monitoring node, partial drops etc. Thus, this work proposes an improved IDS solution named as FBU-NDA for overcoming these issues. It uses a standard centrally controlled monitoring node which listen the transmission of other nodes also. These transmissions had a value compared with standard threshold value to classify actual & misbehaving nodes. At the primary level of work, the approach seems to provide better results in near future.

8. FUTURE WORK

Some problems and concepts that remain unaddressed can be performed in future. Such as with the help of pre-emptive approach more information can be added for exact timely analysis of intrusion & its successful detection with high accuracy. It can also be used for quantitative & qualitative analysis, rank ordering etc. We also embed source code of our proposed scheme in NS2. In our proposed scheme so as to use the benefits of approach like open source.

9. ACKNOWLEDGEMENT

The authors wish to acknowledge college administration for their support & motivation during this research. The authors would also like to thank anonymous referees for their many helpful comments, which have strengthened the paper.

10. REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", in IEEE Transaction on Industrial Electronics, ISSN: 0278-0046, Vol. 60, No 3, March 2013.

[2] S.Mamatha and Dr A Damodaram, "Quantitative Behaviour Based Intrusion Detection System for MANETS", in Proc. of the Intl. Conf. on Advances in Computing and Communication (ICACC), ISBN: 978-981-07-6260-5 doi:10.3850/ 978-981-07-6260-5_59, April 2013.

[3] 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.

[4] 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.

[5] SagarPandiya, RakeshPandit 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.

[6] 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.

[7] MarjanKuchaki Rafsanjani, Ali Movaghar, and FaroukhKoroupi, "Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes", in World Academy of Science, Engineering and Technology, 2008.

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

[9] VinayP.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.

[10] Devi. P and A. Kannammal , "A Hybrid Defense Mechanism for DDoS attacks using Cluster Analysis in MANET", in conference of ICACCI'12, Chennai, Tamil Nadu,, ACM Journal, ISSN: 9781-4503, DOI-1196-0/12/0, July 2012.

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

[12] RakeshShrestha, 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.

[13] FarznehPakzad, MarjanKuchaki Rafsanjani and ArshamBorumandSaeid, "The Improvement Steps of Intrusion Detection System Architectures of MANET", in IJMAS, ISSN: 0973-7545, Vol. 22, Issue S11, 2011.

[14] Amir KhusruAkhtar 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.

[15] 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.

[16] Tushar Sharma, MayankTiwari, Prateekkumar 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.

[17] 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.

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

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

[20] Arun Kumar. R, Abhishek M. K, Tejashwini. A. I, Niranjan J. T and Pradeep R.P, "A Review on Intrusion Detection Systems in MANET", in International Journal of Engineering Science and Innovative Technology (IJESIT), ISSN: 2319-5967, Volume 2, Issue 2, March 2013.

[21] Rohit Sharma and Samridhi Sharma, "Performance Analysis of Intrusion Detection in MANET", in International Journal of Computer Technology and Applications, ISSN: 2229-6093, Vol. 2 (3), 456-462.

[22] MouhannadAlattar, 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.