International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 12 (2018) pp. 10727-10732


# A Method for Reducing the Routing Overhead in Secure Mobile AD HOC Networks

**Kushal joshi1*, and Subodh Mishra2***

[1]*Department of Computer Science, Student of Post Graduate Studies, Medicaps University of Science and Technology, Indore, Madhya Pradesh, India.*

[2]*Department of Computer Science, Faculty Computer Science, Medicaps University of Science and Technology, Indore, Madhya Pradesh, India.*

**Abstract**

In a mobile ad hoc network (MANET), while getting the information about intruder from this method the intruders are identified with some extra security related transmission. The drawback of this method that is identifies once the intruder is detected the direction goes on transmitting some extra packets known as intruder check packets which ultimately increase the routing overhead and degrades the performance of network so there is a need to work upon and to reduce the routing overhead we are going to propose a protocol for reducing routing overhead in secure mobile ad hoc network. In this work the overview of proposed research direction and the objectives of the work are demonstrated.

**Keywords:** Mobile ad hoc networks, RSA algorithm, number of attackers vs. routing overhead.

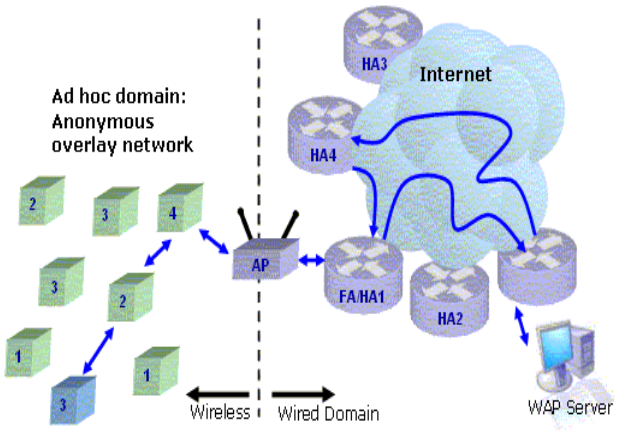


**Figure 1.** Basic topology differentiating network & MANET

## INTRODUCTION

Mobile ad hoc networks (MANETs) consist of a collection of mobile nodes which can move openly. These nodes are without infrastructure and can be dynamically self-organized into arbitrary topology networks. One of the vital challenges in MANETs is the design and implementation of dynamic routing protocols with less overhead and better performance. Ad hoc On-demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) protocols have been proposed for mobile ad hoc network. A MANET is a number of mobile wireless devices which are the structure of the network of any pre-existing infrastructure. All mobile nodes work both as a router as well as host. Fixed broadcast range of wireless interface due to, through intermediate nodes the data traffic has sent packet source to destination over multiple hops. Intrusion detection system (IDS) is the process of detecting the activity of intruders which can affect the process of transmission among the nodes. IDS is considered as the first line of defense for security in MANET. An IDS uses methods and complex techniques for identifying abnormal behaviors. They try to find whether there is any malicious activity or not. The main aim of IDS is to detect the attack before the attacker introduces any harm to the network. In this paper, we are focusing on Reduce the routing overhead & increase the packet delivery ratio in Secure Intrusion Mobile ad hoc networks.

The Network like MANET may or may not be portable. Each user node can be benefitted according to the network id provided by server. Every node in the network must forward the traffic not dependent to its use, and hence It will work as a router. The content of the paper is organized as follows. Section II analyses the related works. Section III discusses various attacks in MANET's. Section IV explains to reduce the routing overhead & increase the packet delivery ratio. Section V describes simulation results and section VI discusses the conclusion.

## RELATED WORKS

Abdulsalam Basabaa et al [1] implemented an intrusion detection system named Adaptive Three Acknowledgments (A3ACKs). The three major problems of Watchdog technique are solved and robust network security is achieved using the proposed method.

Deepa Krishnan [2] has presented an approach which is based on self-adaptive IDS. The salient feature of this approach is that it makes use of the light weight mobile agents.

Elhadi M. Shakshuki et al [3] introduced new IDS called

Enhanced Adaptive Acknowledgment scheme for MANET. Enhanced Adaptive Acknowledgment solves the three major watchdog problems.

Yi Ping et al [4] proposed an intrusion detection system based on timed automata that helps to detect attacks on the dynamic source routing (DSR). The IDS can detect unknown intrusion without trained date or signature but with fewer false alarms.

Vishnu Balan E et al [5] introduced fuzzy based intrusion detection that not only detects attack but also finds the range and extension of attack. Drawback is to reduce the jitter value.

Shengrong Bu et al [6] proposed a scheme that combines authentication and IDS approach in MANET. Multi modal bio metric system is deployed to improve network security.

Adnan Nadeem et al [7] utilized a combination of anomaly-based and knowledge based intrusion detection to protect MANETs from various attacks. But the problem in the IDS is that it causes more harm to network while isolating the attacker in some cases.

Sumit, S et al [9] used effective k-means to isolate attacker nodes from the network in zone routing protocol(ZRP). The drawback of false identification has to be reduced.

Abirami, K.R et al [10] presented a scheme which uses challenge key to detect replica nodes with high accuracy detection rate.

T. Poongothai et al [22] presented intrusion detection technique using machine learning approach. The IDS architecture combines rough set theory and support vector machine to increase the detection rate.

## ATTACKS IN MOBILE AD HOC NETWORKS

Attacks in MANETs are classified into two types, namely active and passive attacks. Passive attack never disrupts the operation of the network. But the active attack disrupts the operation of the network by modifying the data. The various attacks in MANET are discussed below.

Black Hole Attack: In this attack, the malicious node wrongly advertises right paths to destination node during path finding process in the route update messages.

Wormhole Attack: The attacker passes the data from one location to another by creating a tunnel path in the network.

Byzantine Attack: The intermediate nodes involve in colliding the data and degrades the routing services.

Information Disclosure: Confidential information is transferred to unauthorized nodes in the network.

Resource Consumption Attack: The attacker node utilizes the limitedly available resources in the network.

## REDUCE THE ROUTING OVERHEAD

While getting the information about intruder from this method the intruders are identified with some extra security related transmission. The drawback of this method that is identified once the intruder is detected the direction goes on transmitting some extra packets known as intruder check packets which ultimately increase the routing overhead degrades the performance of network so there is a need to work upon and to reduce the routing overhead. The direction of proposed solution will be promoted by sending data and intruder check packets (IC) together. Also the management of Intruder Check (IC) packets transmission will be provided so that the security related transmission can be reduced this will be shown with the help of graph which will decrease the routing overhead.

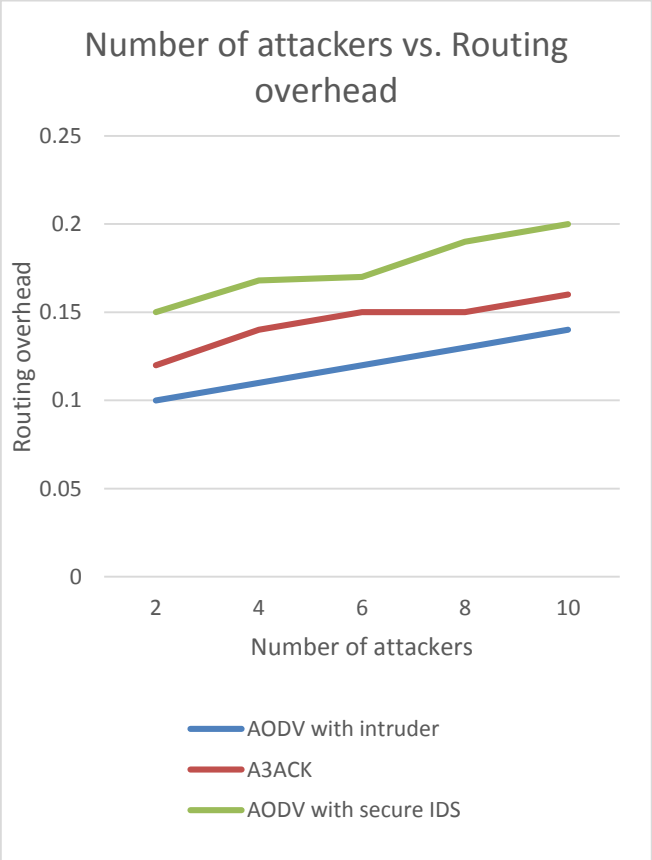


**Figure -2**

Figure 2 Compares the results of number of attackers vs. routing overhead. It clearly shows that secure IDS method have more overhead because of additional intruder check packet compared to existing A3ACK method and AODV with intruders.

## METHODOLOGY

An Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol designed for wireless and mobile ad hoc networks. This protocol establishes routes to destinations on demand and supports both unicast and multicast routing. Figure 3 contains 20 nodes and 10 simultaneous transmissions are going on. IC packets are integrated along with the routing overhead as a parameter is obtain when the probability of intruder is 10% then routing overhead of the proposed algorithm is higher than all the preexisting algorithm.

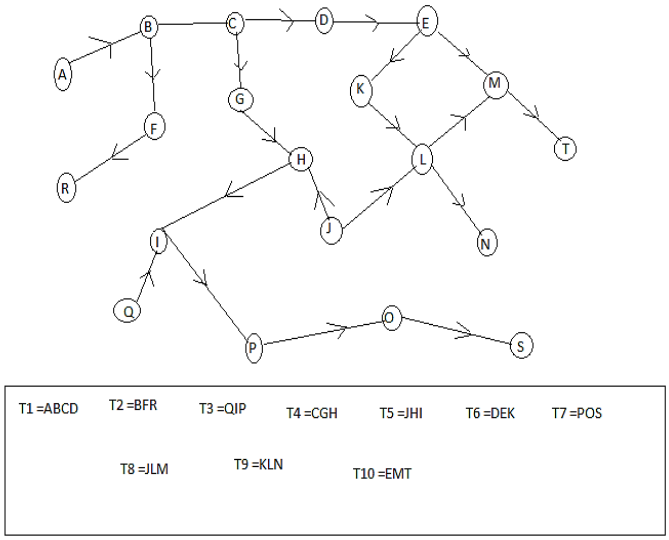


**Figure -3**

## SIMULATION RESULT

The simulation is conducted using Network simulator NS2.34 environment and Ubuntu.

**Table I.** Simulation Configuration

| **Parameter** | **Value** |
|---|---|
| Simulation area | 750 *750 |
| Number of nodes | 20 |
| Payload size | 512 Bytes |
| Routing protocol used | AODV |
| Traffic type | CBR |
| Interference queue length | 150 |
| Simulation time | 100 |

To analyses the performance of our method, we use the following parameters.

**Routing overhead**: It is defined as the ratio of the number of routing related transmissions. In this section we compare the results of AODV with the attack and AODV with secure IDS scheme and A3ACK. Fig. 4,5,6,7,8 compares the results of number of attackers vs. routing overhead. It clearly shows that Out of 10% transmission there is one transmission in which intruder is effecting. simultaneously on 20% transmission, 30% transmission, 40% transmission, 50% transmission.

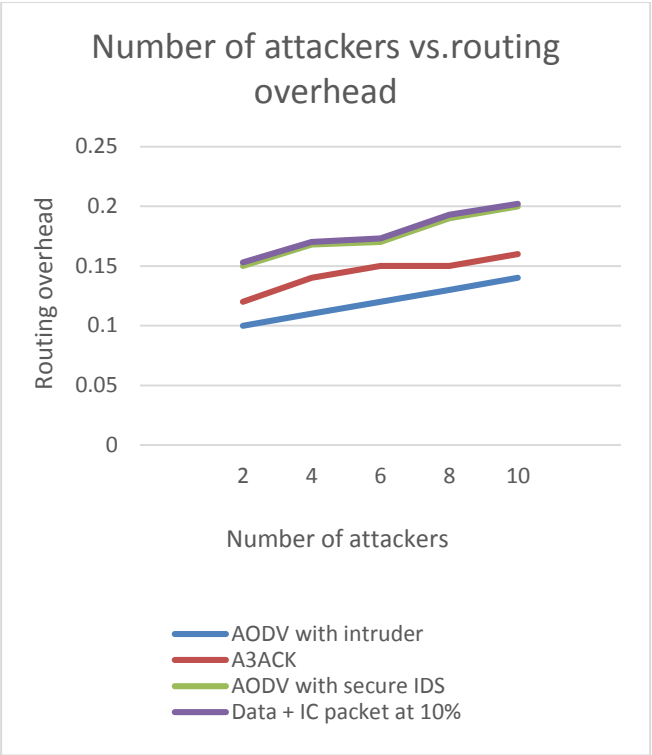


**Figure -4**

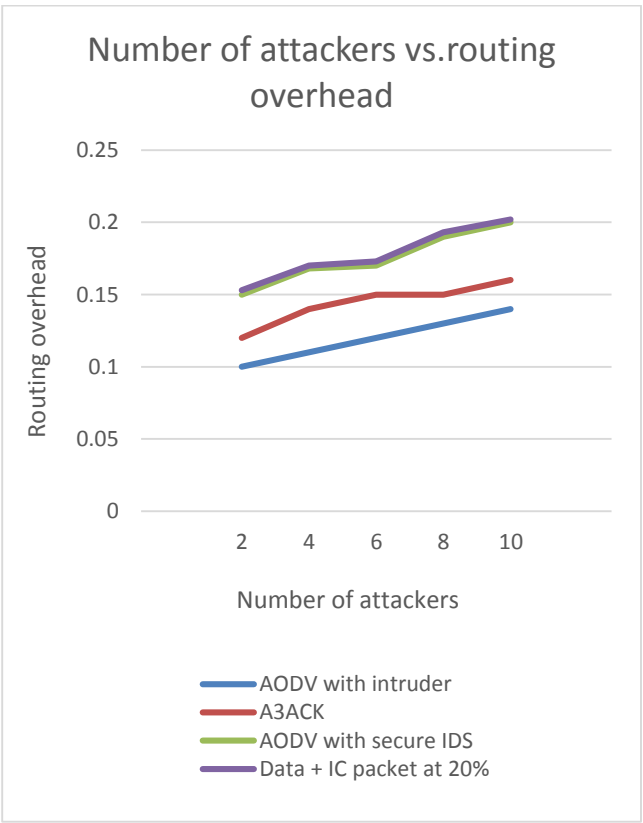


**Figure -5**

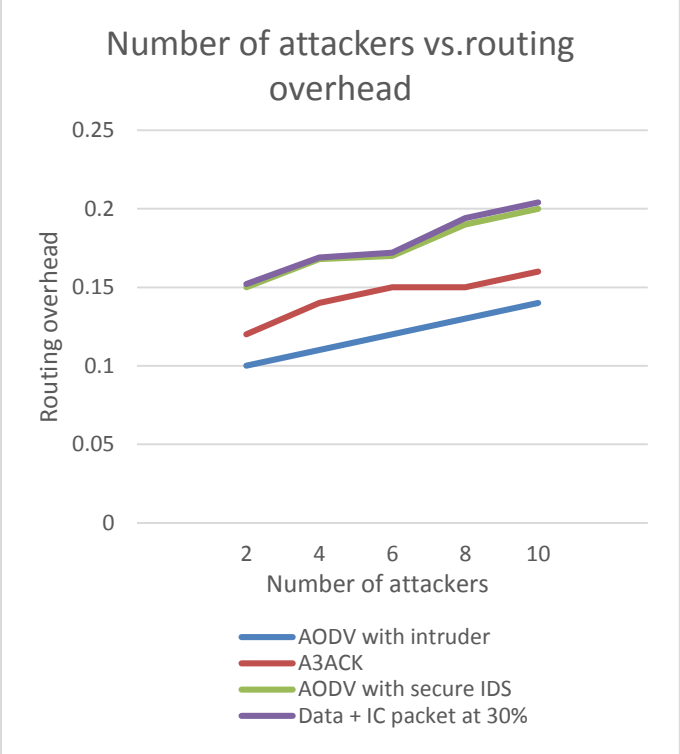


**Figure -6**

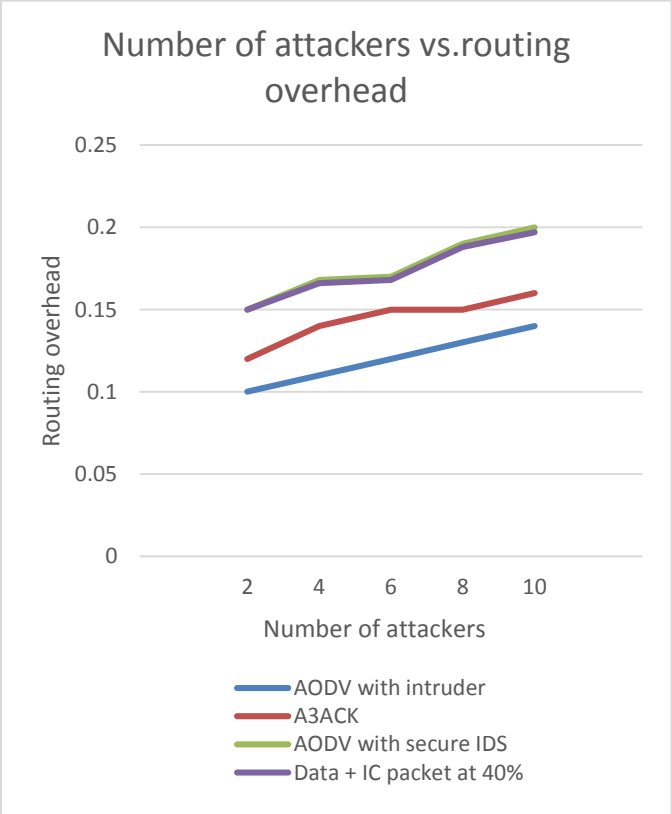


**Figure -7**

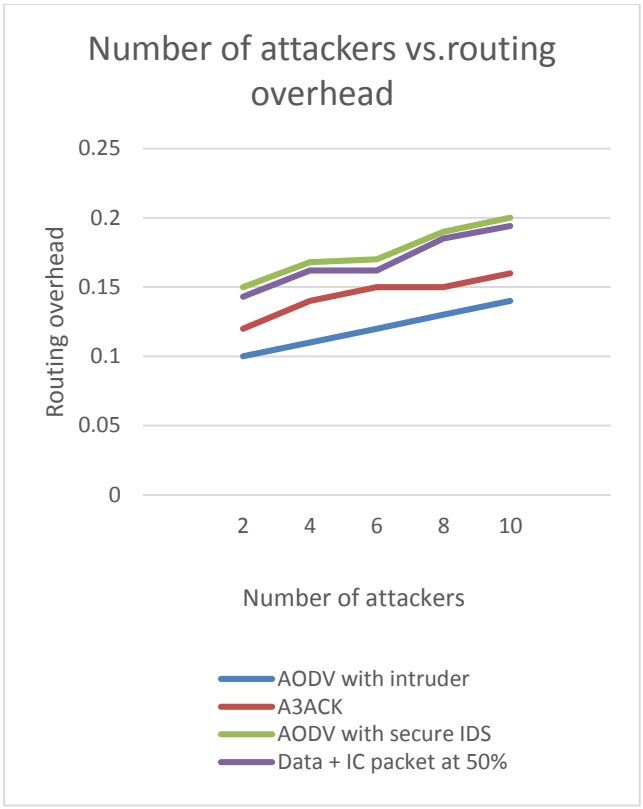


**Figure -8**

## SYSTEM DOMAIN

Implementation of the required system utilizes software and hardware for successfully implementation is listed in this section.

### Framework-

Network simulator (NS2.34) - Network simulators are tools used to simulate discrete events in a network and which helps to predict the behaviors of a computer network. Generally, the simulated networks have entities like links, switches, hubs, applications, etc. Once the simulation model is complete, it is executed to analyze the performance.

### Technology-

RSA algorithm, AD-HOC on demand distance vector routing algorithm.

**Software Specifications**-Operating System (Windows, Ubuntu)

## APPLICATION DOMAIN

Intelligent transportation systems, mobile social networks, emergency deployment, MANET's are widely used in military applications.

## CONCLUSION

Mobile Ad hoc networks are easily affected by various types of network layer attacks. These attacks affect the performance of MANETs drastically. Our proposed Method to reduce the routing overhead in Secure mobile ad hoc network successfully reduce the routing overhead. Results in **Fig -8** clearly shows that our proposed secure method gives better routing overhead in the network Even though packet delivery ratio is on the lower side it is acceptable in future work.

## REFERENCES

[1] Abdulsalam Basabaaa, Tarek Sheltamia and Elhadi Shakshukib, "Implementation of A3ACKs intrusion detection system under various mobility speeds," Procedia Computer Science 32 , 2014, pp. 571 –578.

[2] Deepa Krishnan, "A Distributed Self-Adaptive intrusion detection system for Mobile Ad-hoc Networks using tamper evident mobile agents," Procedia Computer Science 46,2015, pp. 1203 – 1208.

[3] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK— A secure intrusion detection system for MANETs," IEEE Transactions On Industrial Electronics, Vol. 60, No. 3, March 2013.

[4] Yi Ping, Jiang Xinghao, Wu Yue and Liu Ning, "Distributed intrusion detection for mobile ad hoc networks," Journal of Systems Engineering and Electronics, Vol. 19, No. 4, 2008, pp. 851–859.

[5] Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G, "Fuzzy based intrusion detection systems in MANET," 2nd International Symposium on Big Data and Cloud Computing, Procedia Computer Science 50, 2015, pp. 109 – 114.

[6] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, Peter Mason, and Helen Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security Mobile Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 60, No. 3, March 2011.

[7] Adnan Nadeem and Michael Howarth, "Protection of MANETs from a range of attacks using an intrusion detection and prevention system," Telecommunication Systems, Vol. 52, 2015, pp. 2047–2058.

[8] A. Esfandi, "Efficient anomaly intrusion detection system in adhoc networks by mobile agents," IEEE International Conference on Computer Science and Information Technology , July 2010.

[9] Sumit, S., D. Mitra, and D. Gupta, "Proposed intrusion detection on ZRP based MANET by effective k-means clustering method of data mining," IEEE International Conference on Reliability, Optimization and Information Technology, 2014, pp. 156-160.

[10] Abirami, K.R., M.G. Sumithra, and J. Rajasekaran, "An enhanced intrusion detection system for routing attacks in MANET," IEEE International Conference on Advanced Computing and Communication Systems, 2013.

[11] S. Husain, S. C. Gupta,M. Chand , H. L. Mandoria, "A proposed model for intrusion detection system for mobile adhoc network," IEEE International Conference on Computer and Communication Technology, 2010, pp. 99-102.

[12] D. Sandhiya, K. Sangeetha, R.S.Latha, "Adaptive ACKnowledgement technique with key exchange mechanism for MANET," IEEE International Conference on Electronics and Communication Systems , Feb 2014, pp. 1-5.

[13] G. Bourkache, M. Mezghiche, K. Tamine, "A distributed intrusion detection model based on a society of intelligent mobile agents for Ad Hoc Network," IEEE Sixth International Conference on Availability, Reliability and Security , August 2011, pp. 569-572.

[14] K. S. Sujatha, V. Dharmar , R. S. Bhuvaneswaran, "Design of genetic algorithm based IDS for MANET", IEEE International Conference on Recent Trends In Information Technology, April 2012, pp. 28-33.

[15] B. Paramasiva, K. M. Pitchai, "Modeling intrusion detection in mobile ad hoc networks as a non cooperative game," IEEE International Conference on Pattern Recognition, Informatics and Mobile Engineering, 2013, pp. 300-306.

[16] S. Phulre, P. Gautam ; S. K. Mishra, "Implementation of trusted multitier method for intrusion detection in mobile ad hoc networks with DSR algorithm," IEEE Science and Information Conference, 2014, pp. 666-673.

[17] L. P. Rajeswari, R. A. X. Annie ,A. Kannan, "Enhanced intrusion detection techniques for mobile ad hoc networks," IEEE International Conference on Information and Communication Technology in Electrical Sciences, 2007, pp. 1008-1013.

[18] S. Veeraraghavan, S. Bose , K. Anand, A. Kannan, "An intelligent agent based approach for intrusion detection and prevention in Ad Hoc networks," IEEE International Conference on Signal Processing, Communications and Networking, 2007, pp. 534-536.

[19] G. Thamilarasu ; A. Balasubramanian ; S. Mishra ; R. Sridhar, "A cross-layer based intrusion detection approach for wireless ad hoc networks," IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.

[20] Lediona Nishani1, Marenglen Biba, "Machine learning for intrusion detection in MANET:a state-of-the-art survey ," J Intell Inf Syst, Vol. 46, pp. 391-407, 2015.

[21] T. Poongothai ; K. Jayarajan, "A non cooperative game approach for intrusion detection in Mobile Adhoc networks," IEEE International Conference on Computing, Communication and Networking, 2008, pp. 1-4.

[22] T. Poongothai, K. Duraiswamy, "Intrusion detection in mobile Ad Hoc networks using machine learning approach," International Conference on Information Communication and Embedded Systems, 2014, pp. 1-5.

[23] U.Sharmila Begam, Dr.G.Murugaboopath, " A recent secure intrusion detection system for MANETs," International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Special Issue. 1, pp. 54-62, January 2013.

[24] Parthasarathy Velusamy, Murugaboopathi Gurusamy, M.J.Carmel Mary Belinda, "POR: Position based Opportunistic Routing for reliable and efficient data transmission in MANETs," Life Science Journal, Vol. 10, No. 2, 2013.

[25] M. Annie Sharmila, Dr.G. Murugaboopathi, "Contact dissemination based collabarative Watchdog approach to improve selfish node detection in MANETs," International Journal of Emerging Technology and Advanced Engineering, Vol. 3, Special Issue. 1, January 2013. 35567