International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

Consensus Based Algorithm to Detecting Malicious Nodes in Mobile Adhoc Network

R. Sathish Kumar [#1],
Assistant Professor,
Department of Computer Science and Engineering[#1]
Manakula Vinayagar Institute of Technology,
Pondicherry.

T. Dhinesh[#2], V. Kathirresh[#3]
B. Tech,
Department of Computer Science and Engineering[#2,3]
Manakula Vinayagar Institute of Technology,
Pondicherry.

Abstract-- **A wireless network is nothing but a group of nodes that transmit the data from one place to the other, the transmission takes place with the help of ad-hoc network. The network is temporary and dynamic so that the network do not have any security and are vulnerable to attacks at high possible conditions. That attacked nodes are called malicious nodes these nodes act as a selfish nodes which does not pass the data and which results in the decrease of performance. In order to increase the performance the malicious node is detected using the AODV routing protocol and in order prevent the attack, the consensus algorithm is used to prevent the data from getting attacked .In this paper we survey innovated techniques to detect Selfish nodes for MANET. Finally we provide some directions for further research.**

Keywords- AODV, DSR, Routing Overhead, CDSM, VERIFIED, routereply , recvroute , NHN, PHN, MDSAODV

I .INTRODUCTION

A Mobile Ad Hoc network is a self-configuring network that is formed automatically by a collection of mobile nodes without any fixed infrastructure. These wireless devices communicate with each other directly if they are in the same radio communication range [1]. If they are out of the radio range, the communication will require the cooperation of other nodes. Consequently, each mobile node must operate not only as a host but also as a router. Due to these characteristics they are used in many critical applications such as disaster relief, emergency operations, vehicular computing, situational information in the battlefield, mobile offices and many more. In MANETs, one of the most challenging tasks is the security [2]. According to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability MANETs become susceptible to the security attacks. Hence, various attacks of different layers may affect the network.

One of the most famous attacks in MANETs is the Black Hole attack, which can be easily launched on reactive routing protocols like AODV or Dynamic Source Routing (DSR)[4]. In this attack, a malicious node can attract all data packets by falsely claiming a fresh route or shortest route to the destination, without having any active route to the specified destination, and then absorbs them without forwarding it to the destination node [5].

The aim of this paper is to overcome the black hole attack[6]. Therefore, we propose a new approach to eliminate one or multiple black hole nodes on AODV routing protocol. In our approach, the intermediate node forwards the valid route reply to the next node. The invalid routes replies are avoided by intermediate nodes in the overall network. This ratio is checked with a predefined threshold value to detect any malicious behavior. If any misbehavior is found, the detecting node tries to avoid the misbehaving node [7].

A scheme for the routing protocol AODV is proposed to detect and remove Gray Hole and Black Hole Attacks [8]. In this scheme, the intermediate node detects the malicious node sending false routing information by calculating a PEAK value, where the PEAK value is the maximum possible value of the sequence number that any RREP can have in the current state [9]. Then, when this intermediate node receives a RREP having sequence number higher than the calculated PEAK value; it is marked as DO_NOT_CONSIDER [10]. The authors proposed a scheme (so-called DCBA) to identify and mitigate black hole/collaborative black hole attacks in MANETs.

The authors, present a method called Code Division Security Method (CDSM) in order to prevent Black hole attack in MANETs [11]. They consider an additional field of one byte in the packet header to represent the node's code. The approach of Route Reply caching mechanism is used in to overcome the problem of black hole attack. In their approach, they count the RREP received by the source node and then the source chooses the suitable path by ignoring the first RREP.

Our proposed technique differs from the techniques cited above in that it focuses on forwarding only the valid route reply to the next node, even in the case of one or more black hole attacks, by sending twice the same packet reply with the difference of plus one in the sequence number to determine whether the second packet corresponds to the first [12].

II. RELATED WORKS

A Mobile Ad Hoc network is a self-configuring network that is formed automatically by a collection of mobile nodes without any fixed infrastructure. In MANETs, one of the most challenging tasks is the security. According to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability, MANETs become susceptible to the security attacks. One of the most famous attacks in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

MANETs is the Black Hole attack. In this attack, a malicious node can attract all data packets by falsely claiming a fresh route or shortest route to the destination, without having any active route to the specified destination, and then absorbs them without forwarding it to the destination node. The previous work based on a new approach to eliminate one or multiple black hole nodes on AODV routing protocol.

In existing system, to prevent the black hole attack that we had integrated in the AODV routing protocol. Therefore, author slightly modify the recv Reply(Packet *p), recv Request(Packet *p) procedures and the Route Reply (RREP) message According to the original AODV routing protocol, the source node has to broadcast the RREQ packet to find a path to reach the destination node. The destination node, or any intermediate node having the path, can send back the reply to the source node. Then, by default, the source node accepts the first fresh enough RREP packet coming to it. In this approach, like the standard AODV routing protocol, the destination node or intermediate node generates the RREP packet, but it also generates another RREP packet. It is a kind of confirmation of the first packet with a sequence number incremented by one. Therefore, we have two RREP messages from the destination node or an intermediate node that has the route to the destination; one with the normal sequence number and the other with the normal sequence number + 1, and both have the field VERIFIED set to 0. When the intermediate node receives the RREP packet it stores the information about the packet reply, then it checks our appended field VERIFIED if it is set to 0 or 1. If it is 0, that means that our packet is not yet verified or it is an invalid packet. Otherwise the packet is verified and valid and it must be forwarded to the next node. In case of the field VERIFIED is 0 and the intermediate node receives a second route reply message, it must verify if the first route reply's sequence number is the second reply's sequence number minus one; if the verification is true, it sets the field VERIFIED to 1 and forward the packet. Also, when the intermediate node receives another route reply from the malicious node wh ich performs black hole attack with a very high destination sequence number. The same procedure explained will be repeated; and in this case the verification will be false, therefore, the intermediate node leaves the field VERIFIED set to 0 and ignores the packet.

III. LITERATURE SURVEY

A. *Moving target defense mechanisms against source-selective jamming attacks in tactical cognitive radio MANETs,"*

In this mitigation techniques use the concept of address manipulation, which differ from other techniques presented in open literature since our techniques employ de-central architecture rather than a centralized framework and our proposed techniques do not require any extra overhead[13]. Experimental results show that the proposed techniques enable communications in the presence of source selective jamming attacks. When the presence of a source selective jammer blocks transmissions completely, implementing a proposed flipped address mechanism increases the expected number of required transmission attempts only by one in such scenario. The probability that our second approach, random address assignment, fails to solve the correct source MAC address can be as small as 10^{-7} when using accurate parameter selection.

B. *A new approach for detecting and eliminating cooperative black hole nodes in MANET*

In this paper, a new mechanism is presented for detecting and eliminating cooperative malicious nodes in MANET based on Ad hoc On Demand Distance Vector (AODV) routing protocol [14]. In our approach source node checks both Next_ Hop_ Nodes (NHN) and Pervious_ Hop_ Nodes (PHN) of Route Reply generator in order to check the safety of path. By using a Data Routing Information (DRI) table all malicious nodes eliminated from the network. Simulation results show that our approach decreased the processing time and packet overhead in compare with another work. In addition, our approach detects all malicious nodes in a path in each run with no false positive detection.

C. *Defending against Wormhole Attack in MANET*

In this paper, we have survey various techniques dealing with detection of wormhole attack and an approach for wormhole detection and prevention is proposed [15]. A proposed approach is based on the Hash based Compression Function (HCF) which is actually using any secure hash function to compute a value of hash field for RREQ packet. Proposed approach looks very promising compared to other possible solutions in literature survey. All the simulations will be performed in NS2 simulator using AODV reactive routing protocol.

D. *Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis-A Case Study*

In this paper one detection and defence mechanism is proposed to eliminate the intruder that carry out black hole attack by taking decision about safe route on basis of Normal V/S Abnormal (anomaly) activity"[16]. This anti-prevention system checks route reply against fake reply, named as "Malicious Node Detection System for AODV (MDSAODV)". In this paper we analyze the network performance without, with one and multiple (two) malicious nodes, by varying their location. The network performance for MDSAODV is again analyzed under same scenarios through NS-2 simulation.

VI. PROPOSED WORK

1. Overview

This method helps in detecting and preventing the malicious nodes from the wireless networks. It is used to detect the malicious nodes and finds node activity. The performance of AODV is found by introducing some malicious nodes into the network. The throughput, packet drop and the packet delivery ratios are calculated by considering different number of malicious nodes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

2. Maintaining Route

After the route establishment the data is exchanged between the source and destination. But in this mobile ad hoc network nodes are always mobile. If the source nodes moves from the current position then the route discovery is reinitiated as to find the new path using RREQ packet. Or in converse to it if the intermediate nodes or destination nodes move then RERR packet is generated and propagated to the predecessor nodes in the network until it reaches to the source node. When the source node receives the RERR packet then it reinitializes the route or stops sending data.

3. Discovery of Route using AODV

The route in between the nodes is discovered by the entries in routing table. It is ensured that the routing table is the current updated routing table, as the nodes in network are not stable. The network topology always changes since the nodes in mobile adhoc network always moves. According the routing table the data packet is forwarded to the next destination or to the intermediate node. back by the destination node. The RREQ is broadcasted to all the neighboring nodes for particular time limit.

In this time limit the reverse route has to be created between source and destination nodes. If the route is not created within the time limit or the RREQ packet lost somewhere in the network then again the source node sends the RREQ packet and is broadcasted in network. When the reverse route has been established which means the RREQ has reached the destination node then the RREP packet follows the reverse route to reach to the source node. When it reaches to the source node the forward route has been established. When the forward route has been establish now both the nodes can exchange the data between each other.

4. SYSTEM ARCHITECTURE

In fig 1 the system architecture is given below and this method RREQ and RREC is used for transferring the data

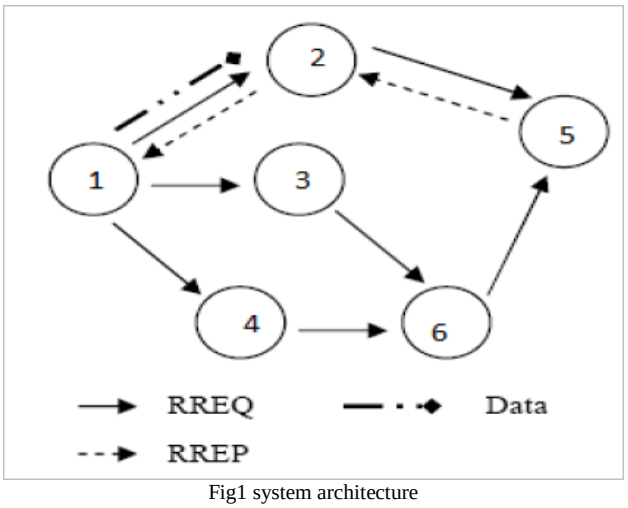

Fig1 system architecture

V. IMPLEMENTATION AND RESULTS

1. Node Deployment

In this simulation scenario consider 27 nodes with random movement within the simulation area 1200 x 1200. The simulation time is 7msec. Initially number of malicious considered are 0 then consider one node. The parameters that are considered for simulation are shown .At first the nodes are distributed among the environment after that they will initialize their position which means server source and destination this only for the identification purpose. Server node is used to monitor the entire nodes, data transmission and packets if the malicious nodes were detected it can send the another route to source. Source node is used to send the data to the destination which transfer the data according to modified AODV routing protocol. By using this method the data can be transferred safely. Node deployment is given in fig 2.

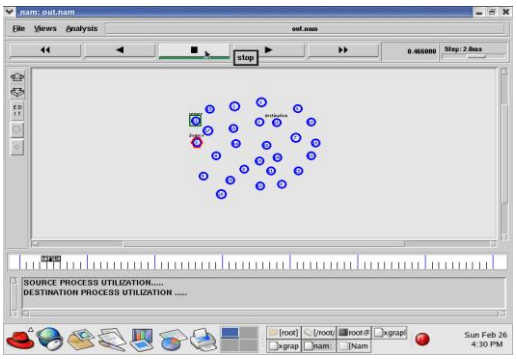

Fig.2 Nodes Deployment

Data transmission is given below. In this method source node transfer the data based on finding the fresh route and maintaining that route. According to that the data is transferred very securely.

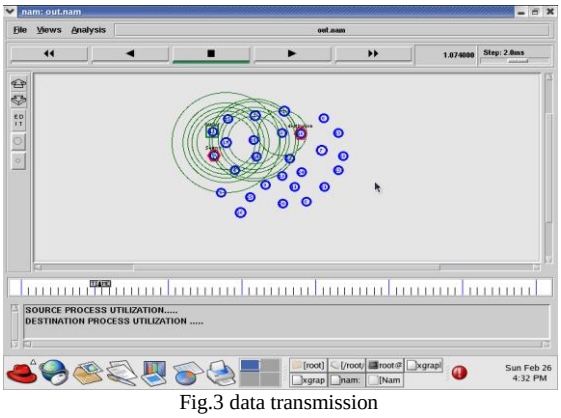

Fig.3 data transmission

1. Malicious node detection

In this module Malicious nodes were detected based on the consensus based algorithm. Due to this malicious node lot of security issues were happened like inappropriate data transmission, data loss, energy consumption, packet dropping. In this method malicious node were detected based on the route reply and route request which identify the malicious node according to the sequence number. If malicious node were detected the server send the another short route to the source. malicious node detection is given in fig 4

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

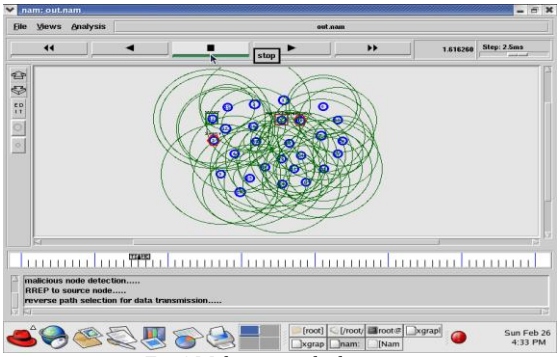

Fig.4:Malicious node detection

3. Secure Data Transmission

According to this method server will send new path to the server when the malicious nodes are detected so that the data is transferred securely from the source to the destination by using the new path. If any malicious node is detected in the new path again the server finds the new path and then the data is transferred securely with the new path. Secure data transmission is given in fig 5.

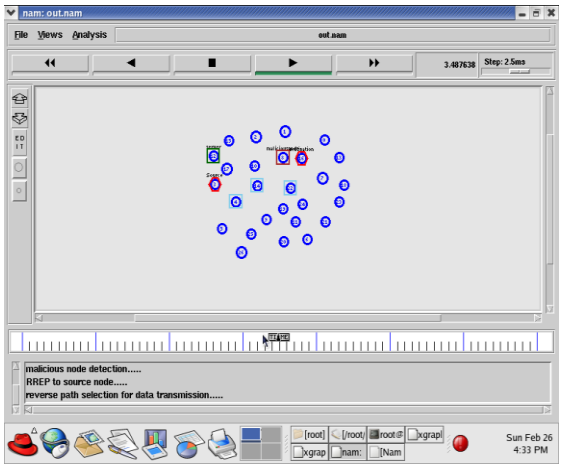

Fig 5 secure data transmission

VI. PERFORMANCE EVALUATION

1. Packet Delivery Ratio

In the Fig. 6 show the packet delivery ratio of consensus algorithm, our solution and AODV under one black hole node and under five black hole attackers when node mobility increases. It is clear from the figures that the performance of our approach is superior over AODV under black hole attack either for one or multiple attackers.

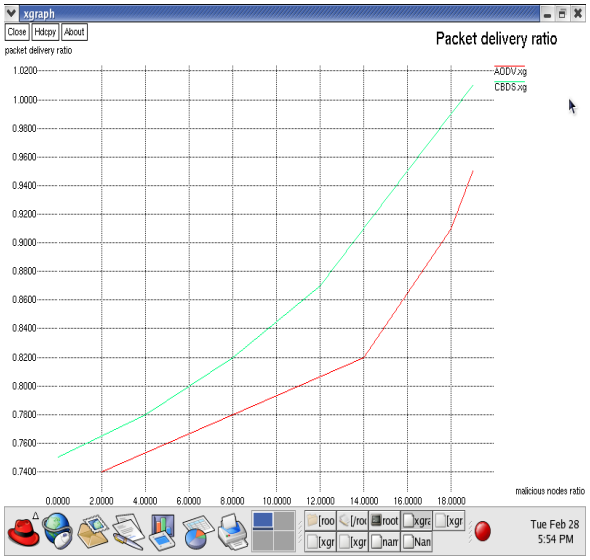

Fig.6 Packet delivery ratio.

2. Routing Overhead

The routing overhead is shown in Fig. 7. In our consensus based algorithm, the routing overhead under one or multiple malicious nodes is slightly higher compared to the standard AODV because of the additional process involved to avoid the selection of malicious nodes. The normalized routing overhead for AODV under black hole attack, whether one or multiple attacks is very high compared to the consensus based algorithm without attack. This is due to the black hole nodes that send false replies to the route request packets which compromise the routing protocol then the protocol starts misbehaving and generating additional routing packets.

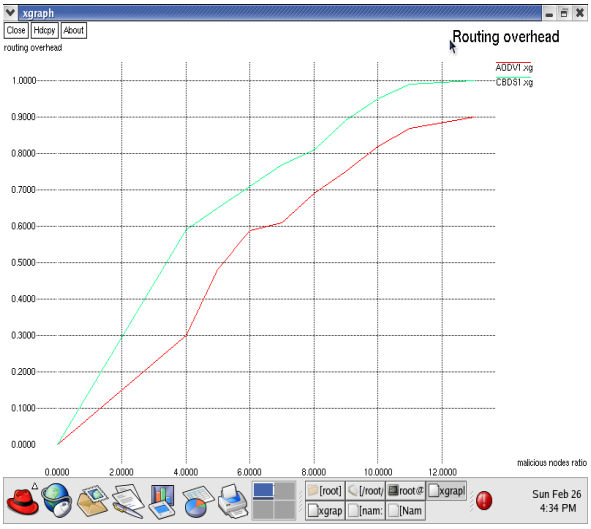

Fig.7 Routing Overhead

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

3.System Throughput

In Fig.8 System Throughput is more efficient that the previous method that is implemented.

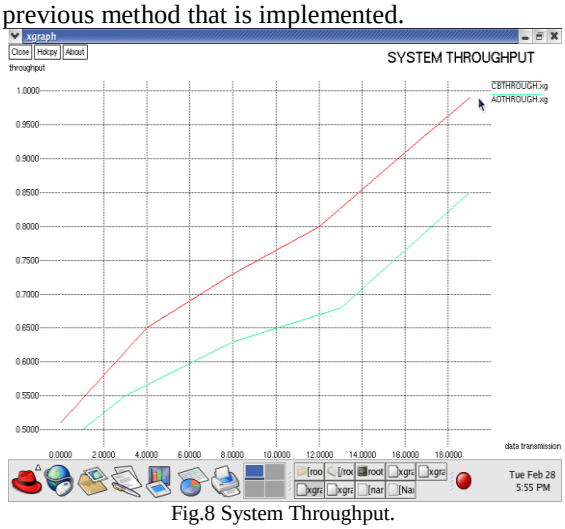

Fig.8 System Throughput.

4.Delay analysis

In the fig.9 Delay analysis is reduces when compared to the previous method that is used.

So consensus based algorithm delay is reduced when compared with AODV method

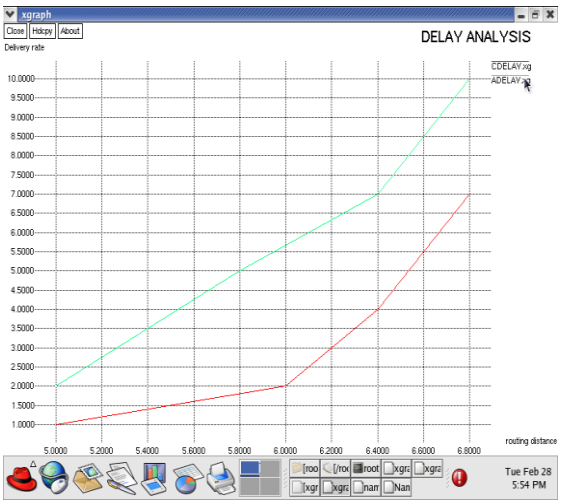

Fig.9 Delay Analysis.

V.CONCLUSION

The techniques proposed are used to eliminate and identify the malicious nodes present in the particular network. Due to the presence of these nodes the per-formance, throughput, packet delivery ratio is reduced and the impact of the AODV protocol is dropped. These attacks make the node malicious so that the transmission of the packets from the source to destination never happens. The Consensus based algorithm helps to detect and prevent the malicious nodes and also provides the successful transmission of the packets between the nodes.

REFERENCES

[1] Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless Network Security* (pp. 103-135). Springer US.

[2] Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). DoS attacks in mobile ad hoc networks: A survey. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* (pp. 535-541). IEEE.

[3] Khatri, S., Sharma, P., Chaudhary, P., & Bijalwan, A. (2015). A Taxonomy of Physical Layer Attacks in MANET. *International Journal of Computer Applications*, *117*(22).

[4] Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In *Proceedings of the 42nd annual Southeast regional conference* (pp. 96-97). ACM.

[5] Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (No. RFC 3561).

[6] Johnson, D. B., & Maltz, D. A. (1996). Dynamic source routing in ad hoc wireless networks. In *Mobile computing* (pp. 153-181). Springer US.

[7] Patel, A. D., Jhaveri, R. H., & Shah, S. N. (2015). I-EDRI Scheme to Mitigate Grayhole Attack in MANETs. In *Intelligent Computing, Communication and Devices* (pp. 39-43). Springer India.

[8] Marttinen, A., Wyglinski, A. M., & Jantti, R. (2014, October). Moving target defense mechanisms against source-selective jamming attacks in tactical cognitive radio MANETs. In *Communications and Network Security (CNS), 2014 IEEE Conference on* (pp. 14-20). IEEE.

[9] Gharehkoolchian, M., Hemmatyar, A. A., & Izadi, M. (2015). Improving Security Issues in MANET AODV Routing Protocol. In *Ad Hoc Networks* (pp. 237-250). Springer International Publishing.

[10] [10] Dorri, A., & Nikdel, H. (2015, May). A new approach for detecting and eliminating cooperative black hole nodes in MANET. In *Information and Knowledge Technology (IKT), 2015 7th Conference on* (pp. 1-6). IEEE.

[11] Patel, A., Patel, N., & Patel, R. (2015, April). Defending against Wormhole Attack in MANET. In *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on* (pp. 674- 678). IEEE.

[12] Gharehkoolchian, M., Hemmatyar, A. A., & Izadi, M. (2015). Improving Security Issues in MANET AODV Routing Protocol. In *Ad Hoc Networks* (pp. 237-250). Springer International Publishing.

[13] Usha, G., & Mahalakshmi, K. (2015). Cross Layer Based Intrusion Detection in MANET Using Intelligent Paradigms. *Networking and Communication Engineering*, *7*(8), 355-360.

[14] Bhandare, A. S., & Patil, S. B. (2015, February). Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis-A Case Study. In*Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on* (pp. 301-305). IEEE.

[15] Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. *Communications Surveys & Tutorials, IEEE*, *15*(4), 2027-2045.

[16] Nadeem, A., & Howarth, M. (2013). Protection of MANETs from a range of attacks using an intrusion detection and prevention system.*Telecommunication Systems*, *52*(4), 2047-2058.

[17] Nadeem, A., & Howarth, M. P. (2014). An intrusion detection & adaptive response mechanism for MANETs. *Ad Hoc Networks*, *13*, 368- 380.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 03, March-2017

[18] Jaisankar, N., Saravanan, R., & Swamy, K. D. (2010). A novel security approach for detecting black hole attack in MANET. In Information Processing and Management (pp. 217-223). Springer Berlin Heidelberg.

[19] Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012, January). A novel approach for grayhole and blackhole attacks in mobile ad hoc networks. In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* (pp. 556-560). IEEE.

[20] Woungang, I., Dhurandher, S. K., Peddi, R. D., & Traore, I. (2013). Mitigating collaborative blackhole attacks on DSR-Based mobile ad hoc networks. In *Foundations and Practice of Security* (pp. 308-323). Springer Berlin Heidelberg.

[21] Patel, M., & Sharma, S. (2013, February). Detection of malicious attack in manet a behavioral approach. In *Advance Computing Conference(IACC), 2013 IEEE 3rd International* (pp. 388-393). IEEE.

[22] Ghathwan, K. I., & Yaakub, A. R. B. (2014). An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET. In *Recent Advances on Soft Computing and Data Mining* (pp. 121-131). Springer International Publishing.

[23] Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2015). A modified algorithm to improve security and performance of AODV protocol against black hole attack. *Wireless Networks*, 1-7.

[24] Ahmad, S. J., Reddy, V. S. K., Damodaram, A., & Krishna, P. R. (2015, January). Detection of Black Hole Attack Using Code Division Security Method. In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2* (pp. 307-314). Springer International Publishing.

[25] Jain, A. K., & Tokekar, V. (2015, January). Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks. In Pervasive Computing (ICPC), 2015 International Conference on (pp. 1-6). IEEE.

[26] Perkins, C. E., & Bhagwat, P. (1994, October). Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers. In ACM SIGCOMM computer communication review (Vol. 24, No. 4, pp. 234-244). ACM.

[27] Issariyakul, T., & Hossain, E. (2011). Introduction to network simulator NS2. Springer

[28] Sathish Kumar. R and Pariselvam .S , ―Formative Impact of Gauss Markov Mobility Model on Data Availability in MANET, Asian Journal of Information Technology 11(3): 108-116 ,2012.

[29] Sathish Kumar.R, Aktharunissa.A, Koperundevi.S, S. Suganthi"Enhanced Trust Based Architecture in MANET using AODV Protocol to Eliminate Packet Dropping Attacks", International Journal of Engineering Trends and Technology (IJETT), V34(1),21-27 April 2016. ISSN:2231-5381.