Implementation of Secure and Energy Efficient Routing Protocol for Mobile Adhoc Network

Mukesh Kumar Raigar[1], Mr. Manish Dubey[2]
M. Tech Scholar[1] – A. I. E. T, Department of CSE, RTU, Kota, India
Associate Professor[2]– A. I. E. T, Department of CSE, RTU, Kota, India
chorotiamukeshkumar@gmail.com[1], manishdubeycse@gmail.com[2]

Abstract – Mobile adhoc network are networks consisting of spatially distributed autonomous sensors, which are capable of sensing the physical or environmental conditions and have set of applications in various domains. But MANET is also prone to various active and passive attacks due to the lack of security mechanism, centralized management in routing protocol and. The prime task of WSN is to sense and collect information, process and transmit to the sink. One of the major security threats in MANET is attacks; attacks may be active or passive. First of all implementation of reference work carried out in NS 2 environment for various numbers of nodes in the range from 10 to 50 followed by integration of attacker node. In our research work specifically black hole attack has been taken to see the impact on network parameters. To overcome such active attacks an advanced Ad hoc On-Demand Distance Vector routing protocol techniques incorporated hash function with security algorithm so that data cannot be accessed by unauthorized person. Network matrices are improved by implementing advanced AODV routing protocol. In the distributed network trust among various sensing nodes is a powerful tool to increase the performance of device networks. In our research work depth analysis carried out on the security and trust communication between the device nodes with routing techniques to discover and prevent information packet from the being exposed to black hole attack. Further various mobility pattern can be investigated with different attacks.

***Key Words –** MANET, Routing Protocol, Active Attack, Passive Attack, Node, Adhoc*

*****

I. INTRODUCTION

Wireless Sensor Networks are emerging as one of the prevailing technologies of the future due to their wide range of applications in military and civilian domains. Due to their operating nature, they are often unattended and hence prone to different types of novel attacks. Nowadays, wireless networks play a vital role in information technology. An ad-hoc network is considered as a decentralized type of wireless network. A mobile ad-hoc network is a type of ad-hoc network where nodes are free to move around. The MANET consists of a number of mobile nodes that can connect to each other over multi-hop wireless links on an ad-hoc basis. MANETs are self-organizing, self-configuring as well as self-healing without requiring any infrastructure or central administration [3].

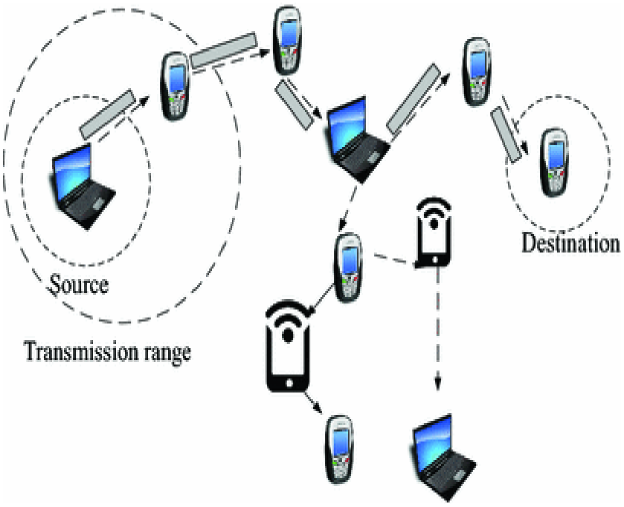

Figure 1 Mobile Ad hoc Networks

Due to limited transmission range, a mobile node may not communicate with a distant node directly. However, in MANET each node acts as a relay node. This allows a mobile node communicating with a distant node over multi-hop link. A MANET is considered as an excellent candidate for a number of applications ranging from battlefield communication, meeting events, conferences, and emergency search-rescue operations. MANET nodes can arbitrarily be located within an area and are free to move. The movement of MANET nodes changes the network topology dynamically. MANET nodes adapt to the changing topology by discovering new neighbours and establishing new routes to destinations [5]. When a node wants to send data to a remote node, first, it finds a set of relay nodes between itself and the remote node. The process of finding the optimal set of relay nodes between the source node and the destination node is called route discovery. Node mobility, limited battery power and the error-prone nature of wireless links are the main challenges in designing an efficient routing protocol in MANETs. A self organizing adaptive collection of such devices connected with wireless links is said to be an Adhoc network.

II. LITERATURE SURVEY

Abhilash Singh et al: MANET is temporary, dynamic network and an infrastructure less. In the domain of CN, MANET has wide set of application. On other hand it is also severely prone to diverse attacks due dynamic topology and infrastructure less. There are so many attacks for example gray attack, Sybil attack, wormhole attack. Black hole attack is one of the most danger security threats in MANET. In black hole attack, false node is introduced in the network with highest probability and this node capture the information from source and blocks this information to reach destination node and send an acknowledgment to source node that your data has been sent to destination node perfectly. In this paper, black hole attack on MANET is executed and effects of the black hole attack analyzed based on diverse parameters [1].

Y. Pavan Kumar Guptha et al: WSN having huge of application as per requirements and in these days we can say that it is our crucial part of our life. In earlier times wired devices are used but with pace of time new innovation came into existence into real world which made our life so comfortable. In the same way MANET did the same way and wired devices replaced by wireless technology. A cluster is formed between various nodes and data is transmitted from one device to other node in form of packet. In this research an extreme analysis executed on security and trust communication between various nodes carried out so that black hole can not affect the data which have to send destination node. Besides this article concludes with a comparative analysis between present works [2].

Z. Zheng et al: In this paper, we suggest an energy-saving location-alert clone distinguish protocol in WSN where nodes are in abundant, which can assurance victorious clone attack detection and maintain novel network lifetime. In this research, theoretically we demonstrate that suggested protocol can attain 100% clone perceive probability with trustful evidences. We further carried out work by analyzing clone notice performance with lied witnesses and proved that clone detection probability still attain 98% when 10% of witnesses are compromised [3].

M. Dong et al.: This paper gives an investigation idea to attain requirements of a recognize application through horse trading between the energy consumption and source-to-sink (S2S) transport delay under reliability restraint WSN. A novel data collecting protocol named Broadcasting Combined with Multi-NACK/ACK (BCMN/A) protocol is suggested based on the investigation approach. The BCMN/A protocol is examined by theoretical method as well as ample simulations and these consequences indicate that our suggested protocol jointly maximize the network over all lifetime and transport delay under network genuine constraint [4].

C. Zhu et al.: This paper presents a novel authenticated trust and reputation calculation and management (ATRCM) system for CC-WSN integration. The advance ATRCM system attain the following three functions: 1) Authenticating between CSP and SNP to avoid false imitation attacks; 2) To compute and supervise trust and integrity regarding service of CSP and SNP; and 3) To assist CSU to select desirable CSP and assisting CSP in selecting suitable SNP. Deep analysis and simulation design as well as further various functionality evaluation results are depicted to exhibit the effectiveness of ATRCM, followed with system security analysis [5].

III. METHODOLOGY

Our research work is categorized into three modules which depict existed work followed by integrating malicious node and then followed by secure AODV protocol and comparative analysis of network matrices.

Module 1

1. Generating Network Topology using no. of Nodes 10, 20, 30, 40, 50 using congestion window.
2. Using AODV routing Protocol in these topologies.
3. Calculate the Performance parameters like PDR, Throughput, Delay, Energy, and Overhead

Module 2

1. After that integrate a malicious node (attacker node) in AODV routing protocol.
2. Integrate Black hole attack in AODV routing Protocol
3. Calculate the Performance parameters like PDR, Throughput, Delay, Energy, and Overhead.

Module 3: (Proposed Work)

1. After that integrate a Proposed Method (Hash Function, RSA Cryptography using generating a public & private key for encryption & Decryption) in Secure AODV routing protocol.
2. Compare the Both base model and proposed model
3. Calculate the Performance parameters like PDR, Throughput, Delay, Energy, and Overhead

AODV is most popular routing protocol for MANETs. In this protocol, a node discovers a route on demand, i.e., only when it is needed, and caches it. Network wide flooding is used to discover the routes. This protocol requires that nodes maintain local connectivity information by sending periodic local broadcast messages known as hello messages. Through these hello messages a node becomes aware of its neighbors or nodes in its radio range. When a source node wants to send a message to a destination node and a route to the destination is not available in the cache, it initiates a path discovery process by broadcasting a route request (RREQ) packet. When a node receives a RREQ packet it checks whether it has received the same packet before, if it has then it discards the packet. The node then determines whether it has a route to the destination node in its cache. If it cannot satisfy the route request of the source then it rebroadcasts the packet after setting up a reverse path to the source. To set up a reverse path, a node records the address of the neighbor from which it received the first copy of RREQ as the next hop to the source. Eventually a RREQ arrives at a node (possibly the destination itself) that possesses a current route to the destination. Then node unicasts a route reply (RREP) packet back to the source. As the RREP travels back to the source, each node along the path sets up a forward pointer to the node from which the RREP was received as the next hop to the destination and updates its timeout information for the route entries to the source and destination. Nodes that are not part of the path determined by the RREP, timeout after ACTIVE_ROUTE_TIMEOUT and delete the reverse path to the source.

When a node detects that a destination node is unreachable (a link failure is detected either by failure to receive hello messages or a link-layer acknowledgement), it propagates to all the active neighbors a route error (RERR) packet for the failed routes for which the node was the next hop.

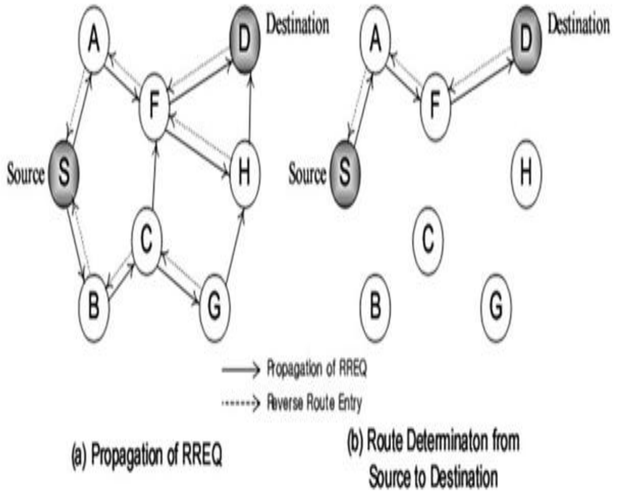

Figure 2 AODV routing protocol procedures

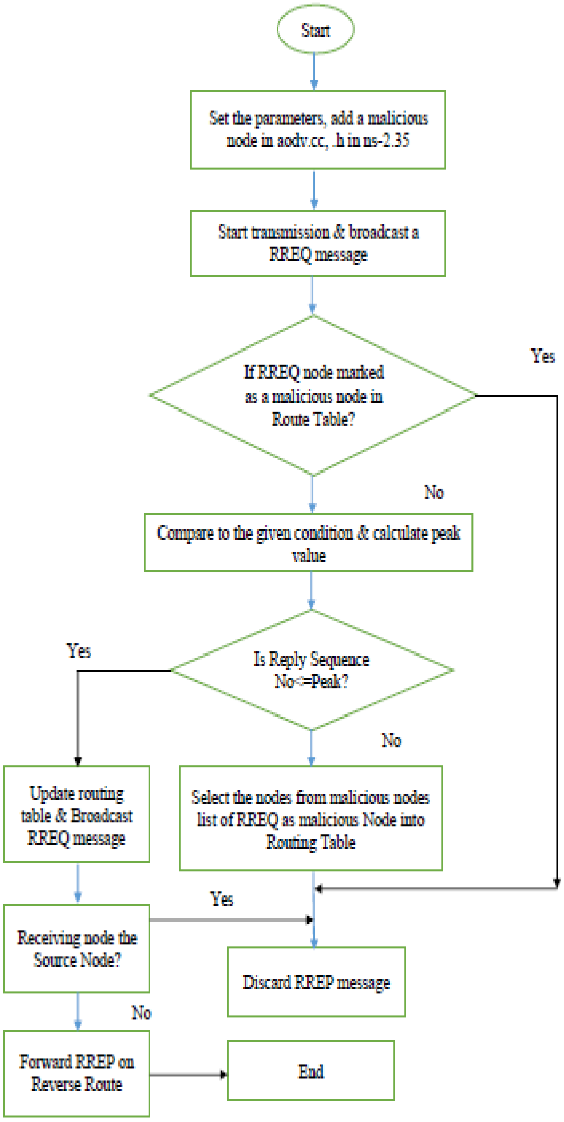
Start
Set the parameters, add a malicious node in aodv.cc, .h in ns-2.35
Start transmission & broadcast a RREQ message
If RREQ node marked as a malicious node in Route Table?
Yes
No
Compare to the given condition & calculate peak value
Is Reply Sequence No<=Peak?
Yes
No
Update routing table & Broadcast RREQ message
Select the nodes from malicious nodes list of RREQ as malicious Node into Routing Table
Yes
Receiving node the Source Node?
Discard RREP message
No
Forward RREP on Reverse Route
End

Figure 3 Proposed work flow-chart

Discovery of Route

A source node that needs to send data to a destination node triggers route discovery mechanism by broadcasting a special control packet, called Route Request (RREQ), to its neighbours who then rebroadcast the RREQ packet to their neighbours. The process continues until the RREQ packet arrives at the destination node. The destination node sends a control packet called Route Reply (RREP) that follows the path of RREQ in the reverse direction and informs the source node that a route has been established. Since every node on receiving the RREQ for the first time rebroadcasts it, it requires T- 2 rebroadcasts in a network of T nodes assuming the destination is reachable. This kind of broadcasting is called pure flooding [11] and is depicted in simplified form in Figure

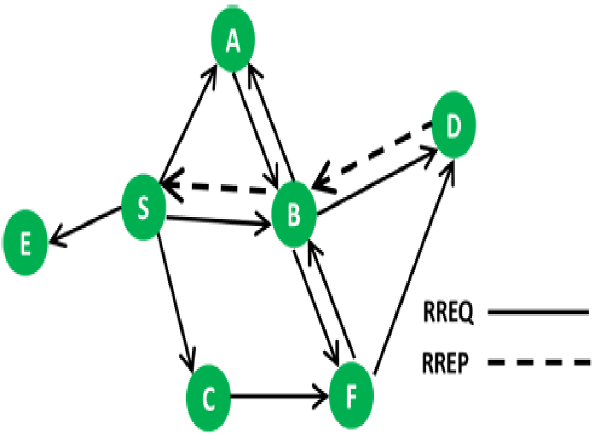

Figure 4 Route discovery process between nodes S and D

IV. RESULT AND DISCUSSION

SOFTWARE: There are various software available to execute networking model. In this section, we will depicts how the proposed protocol performs better in terms of energy efficiency, Throughput, PDR, average end-to-end delay of WSN. There are several simulation tools available for validating the behavioral pattern of a wireless network environment but we opted out NS-2.35 as our tool in simulating the proposed protocol.

Simulation Tool	**NS-2.35**
Operating System	Ubuntu 12.04
No. of Nodes	10,20,30,40,50
MAC/PHY layer	IEEE 802.11
Antenna model	Omni directional
Interface queue size	50 packets
Data payload	512 bytes
Pause time	20 seconds
Channel bandwidth (data)	12Mbps

ISSN: 2454-4248

Transmission range	250m
Examined protocol	AODV
Interface Queue Type	Queue/Drop Tail/PriQueue
Mobility model	Random way point
Simulation area	500M*500M
Link Layer Type	LL
Rx Power	0.6
Tx Power	0.6
Data Rate	200k
Simulation Time	100 sec

In adhoc network security is prime concern these days because adhoc network are vulnerable to attack therefore need to secure are network from unauthorized person so that information can be protected. Attacks are categorized into two types

- Active attack
- Passive Attack

In these types further various types of attack available. In this research paper AODV protocol is used. This paper depicts impact of black hole attack on AODV protocol and to overcome this proposed protocol is implemented with security.

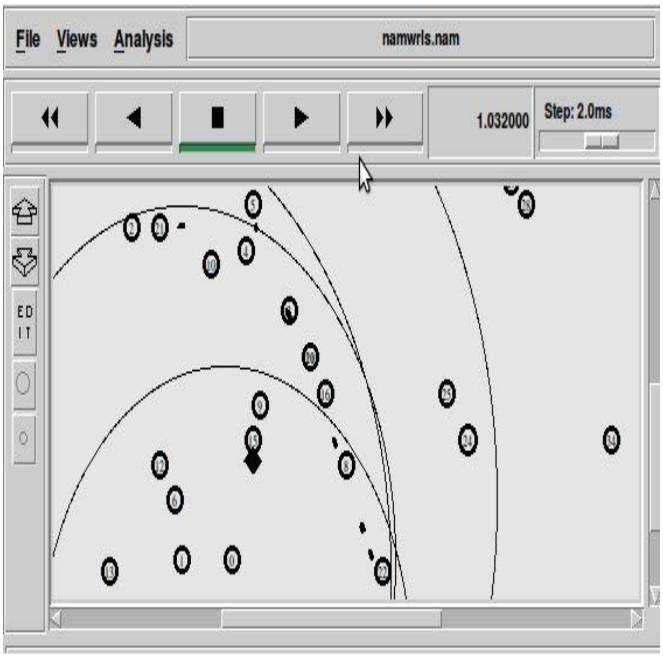

Figure 5 Network animations for 40 node and communication started between nodes

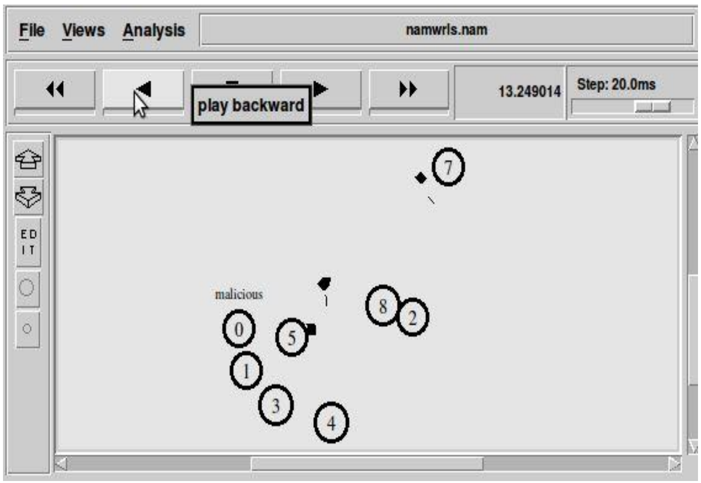

Figure 6 Communication between nodes and dropped packet

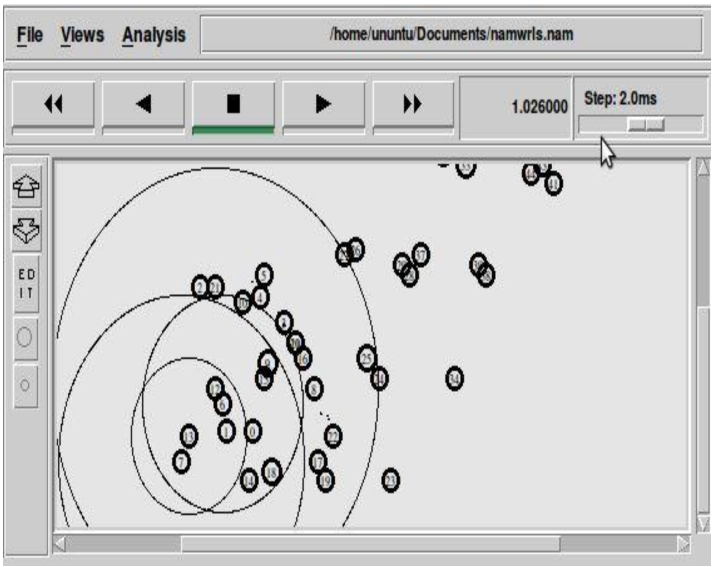

Figure 7 Attack of malicious node in a network of 50 nodes

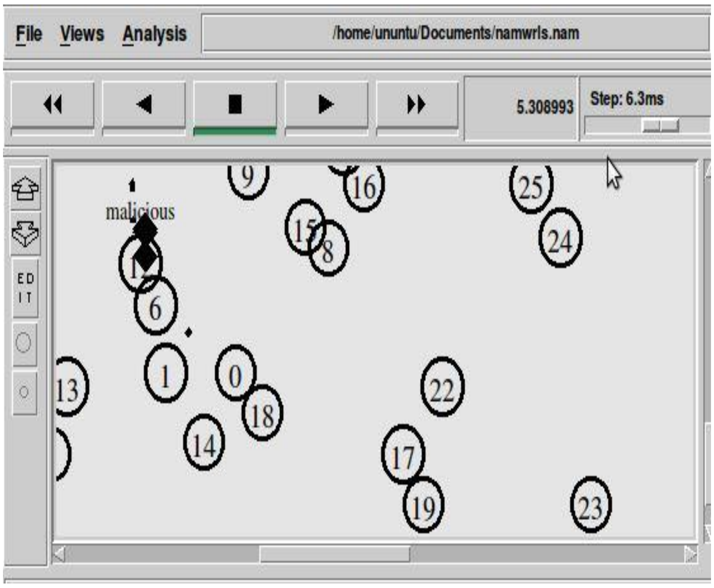

Figure 8 Dynamic malicious node in a network of 50 nodes and loss of packet

Average End-to-End Delay –The average time packets take to traverse the network. This is the time from the generation of the packet by the sender up to send at the destination application layer and expressed in second. It therefore include all the delay in the network such as buffer Queue, transmission and delay induced by routing protocol activities and MAC control data exchanges.

End to End delay = [(Sum of Individual data packet delay) / (Total number of data Packets delivered)]

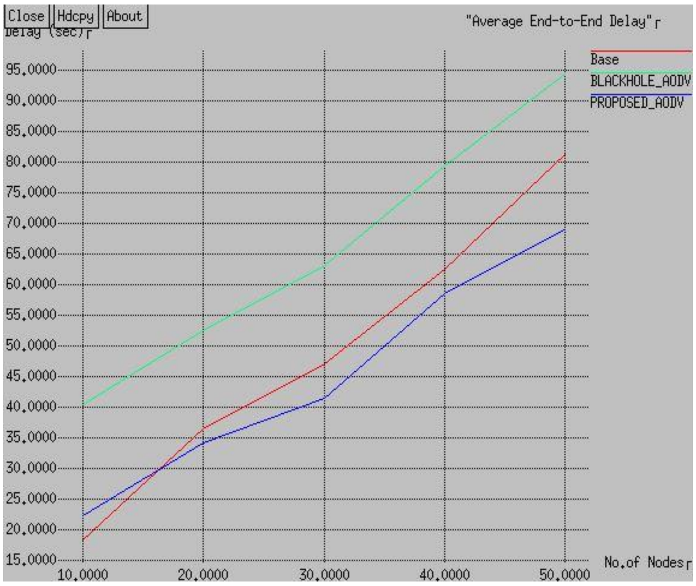

Figure 9 Average end-to-end delay comparison

Energy Consumption – Energy is converted in joules by multiplying power with time. Graph below shows the energy consumed by mobile nodes in WSN. Energy consumption represented in Joule per Second.

Energy Consumption = [(Sum of Energy expended by each node) / (Total number of data packets delivered)]

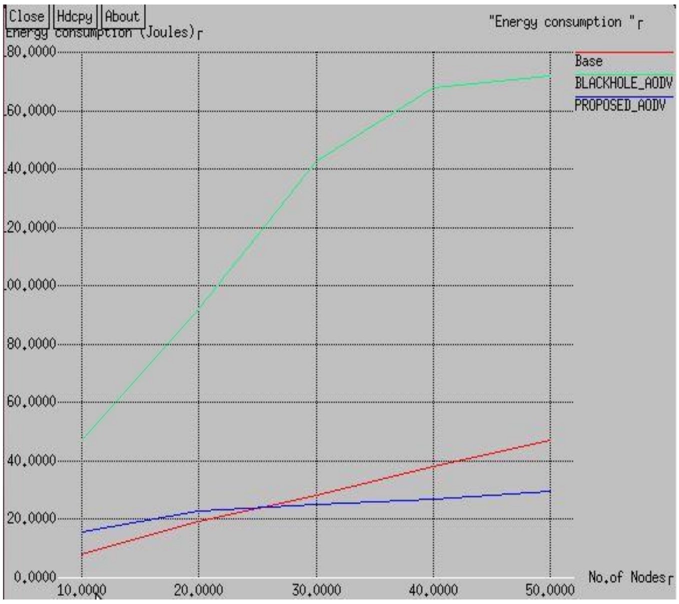

Figure 10 Energy Consumption comparison

Packet Delivery Ratio (PDR) – The ratio between the numbers of packets delivered to receiver to the number of packets sent by the source is called as Packet Delivery Ratio. It denotes the maximum throughput a network can achieve. A high average packet delivery ratio is desired in the network

Packet Delivery Ratio = (Packets Received / Packets Generated) * 100

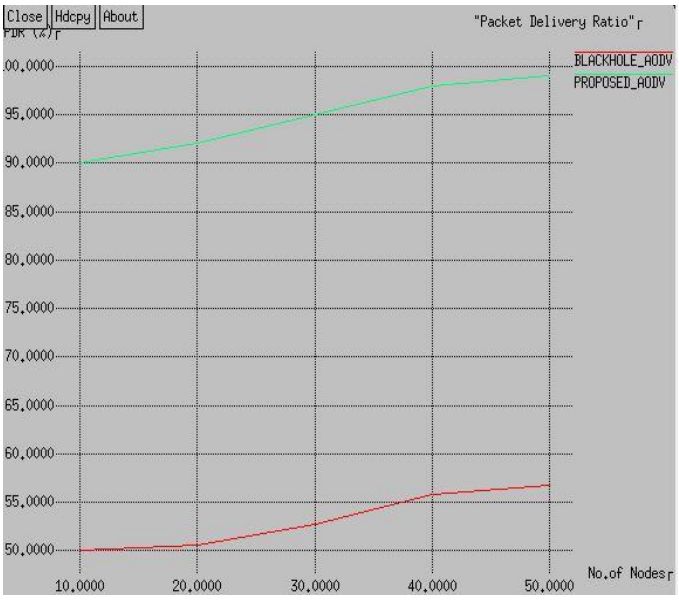

Figure 11 Packet Delivery Ratio comparison

Average Throughput – The ratio of total amount of data that reaches from a sender to receiver to the time for the receiver to get the last packet is referred as Throughput. It includes frequent topology changes, unreliable communication of messages, limited bandwidth and insufficient energy in WSN's. A network with high average throughput is desirable.

Throughput = (Number of data packets received*Packet size*8) / Simulation time

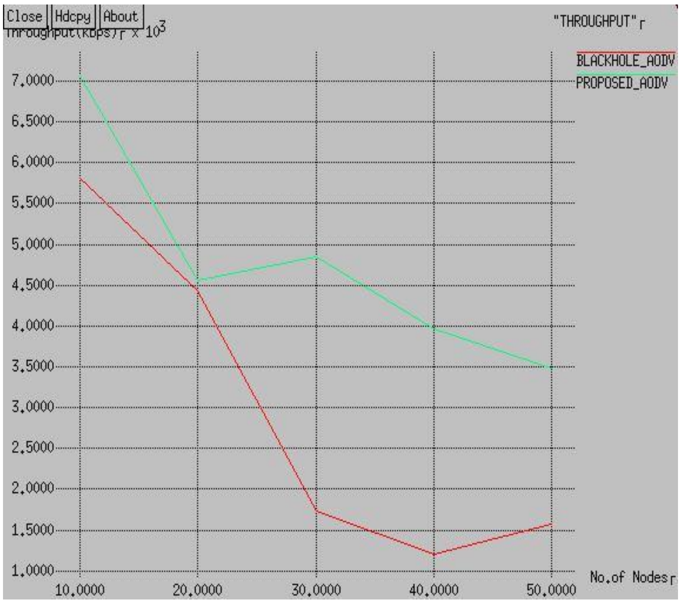

Figure 12 Throughput comparison

HOP - In computer networking, including the Internet, a hop occurs when a packet is passed from one network segment to the next. Data packets pass through routers as they travel between source and destination. The hop count refers to the number of intermediate devices through which data must pass between source and destination

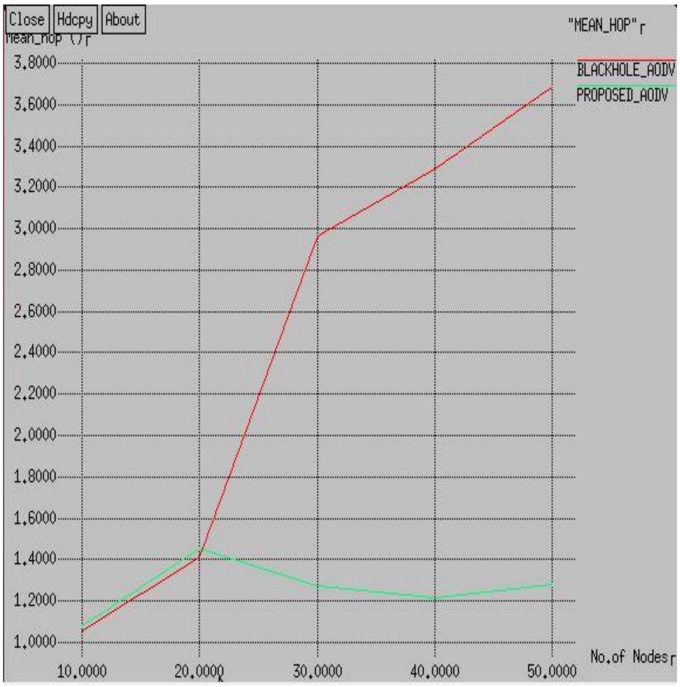

Figure 13 Comparison of Mean hope

V. CONCLUSION

Mobile adhoc network is severe prone to black hole attack and this security threat is well-known in wireless mobile ad hoc networks. The unauthorized person utilizes loophole to fetch out their malicious behaviors because the route discovery process is mandatory and unavoidable. By categorizing the overall WSN system into a few constituents, components of each constituent were extracted in terms of their dominant factors, followed by a mathematical formula as a total energy cost function in terms of their constituents. The prime task of WSN is to sense and collect information, process and transmit to the sink. One of the major security threats in MANET is attacks; attacks may be active or passive. First of all implementation of reference work carried out in NS 2 environment for various numbers of nodes in the range from 10 to 50. Thereafter integration of attacker node executed in implemented reference work. In our research work specifically black hole attack has been taken to see the impact on network parameters. To overcome such active attacks an advanced Ad hoc On-Demand Distance Vector routing protocol techniques incorporated hash function with security algorithm so that data cannot be accessed by unauthorized person. Network matrices are improved by implementing advanced AODV routing protocol and improved parameters. In future work, different mobility patterns under diverse network circumstances can be considered and impact of various attacks can be investigated.

REFERENCES

[1]. Abhilash Singh, Kaustav Pratim Kalita, Smriti Priya Medhi, " Black Hole Attacks on MANETS and its Effects", Proceedings of the 12th INDIACom; INDIACom-2018 5th 2018 International Conference on "Computing for Sustainable Global Development", 14th – 16th March, 2018

[2]. Y. Pavan Kumar Guptha , M. Madhu, "Improving security and detecting blak hole attack in wireless sensor network", International journal of professional engineering studies, Volume 8 , Issue 5, AUG 2017

[3]. Z. Zheng, A. Liu, L. Cai, Lin X. Cai, Zhigang Chen, Xuemin (Sherman) Shen, "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks," IEEE Transactions on Mobile Computing vol. 15, no. 5, pp. 1130-1143, 2016

[4]. M. Dong, K. Ota, A. Liu, Anfeng Liu and Minyi Guo, "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016

[5]. C. Zhu, H. Nicanfar, V. C. M. Leung, Laurence T. Yang, "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.

[6]. A. Liu, M. Dong, K. Ota, Jun Long, "PHACK : An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no. 12, pp. 30942-30963, 2015

[7]. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.

[8]. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency," IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2014.

[9]. S. He, J. Chen, F. Jiang, et al. "Energy provisioning in wireless rechargeable sensor networks," IEEE transactions on mobile computing, vol. 12, no. 10, pp. 1931-1942, 2013

[10]. A. Liu, X. Jin, G. Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network," Information Sciences, vol. 230, pp.197-226, 2013.

[11]. T. Shu, M. Krunz, S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954, 2010.