Mohammed Shahbaaz * et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.5, Issue No.5, August - September 2017, 7184-7190.

Preventing Black Hole Attack from Manets Using Secrete Key

MOHAMMED SHAHBAAZ
M.Tech Student,CSE Branch, Nawab Shah Alam Khan College of Engineering & Technology

Dr. CHANDRA NAIK M
Professor, Nawab Shah Alam Khan College of Engineering &Technology,New Malakpet, Hyderabad, Telangana State, India-500024

Dr. G. SAMBASIVA RAO
Professor, Nawab Shah Alam Khan College of Engineering &Technology,New Malakpet, Hyderabad, Telangana State, India-500024

Abstract: **MANETs system made out of remote portable device that communicates by transferring on wireless medium. This system & portrayed by absence of infrastructure, without focal facilitator and central assets. Communication is conceivable by device in a system are helpful; however, it is not generally valid in disseminated compelled asset condition. Hacker can play out the malicious exercises by not following directing convention of network layer protocols, one such attack is black hole attack. In which black hole device control the routing messages and pull in the correspondence data towards it and after that drop the data. Earlier works identifies and prevent black hole attack by observing the nodes in a network, which is not practical arrangement in hostile environment. The proposed technique mitigates Black Hole Attack from routing path in MANETs by Secret Key and Hashing. Analysis of our results demonstrates that our proposed technique precisely removes the black hole attack and extend the performance of network.**

Keywords: **Manet; Black Hole; Secrete Key and Ns-2 Simulator;**

I. INTRODUCTION

Wireless mobile ad-hoc network technology is designed for the establishment of a network anywhere and anytime, characterized by lack of infrastructure, clients in a network free to move and organize themselves in an arbiter fashion. Communication may have multiple links and heterogeneous radio, can operate in a stand-alone fashion, with self configured & self maintenance. It is a wireless network consist of collection of heterogeneous mobile devises (nodes) which are connected by a dynamically varying network topology without fixed infrastructure and absence of central coordinator or base station where network intelligence placeless inside every node thus nodes in a network act as a router as well as host which means MANETs behave as a peer to peer network. The connectivity between nodes may have a multiple links and heterogeneous radio and can operate in a standalone fashion. Due to characteristics of MANETs well suited a situation where infrastructure is difficult to setup, cost or time effective.

The design, development, performance of MANETs majorly include in routing, QoS, Security, multicasting, service discovery, scalability & Resource management (energy, bandwidth, delay and battery power). The QoS design issue is inherently related with MANET's applications. Qos is the performance level of service which is offered by the network to user in case of QoS routing process it has to provide end to end loop free path with ensure the necessary QoS parameters like bandwidth, delay, jitter, availability and resources has met. Depending up on the application QoS parameter varies.

- Real Time Traffic: - Bandwidth, Delay
- Group Communication: - Battery Life
- Emergency Services: -Network Availability
- Security

Routing, QoS & security is challenging in MANETs compared to infrastructure network due to its characteristics like dynamic network topology, absence of pre established infrastructure for central administration, mobility of nodes, resource constraint, error prone channels and hidden, expose node problem. Routing in MANETs is an active research area in recent years; number of routing protocols has been developed. Routing protocols are useful when they offer acceptable communication services like route discovery time, communication throughput, end to end delay, and packet loss

Energy-Efficient routing is another effective factor for MANETs routing due to its energy Constraint characteristic so as to reducing the energy cost during data communication. Routing protocol aim is to just finding energy consumption during end to

end packet travelling is not reliable routing but it also considers reliable links and residual energy of nodes which not only improve QoS but also improve life time of network. Various routing protocols have been proposed which aim to improve reliability, energy efficiency and life time of network.

In any MANET's application secure communication is important; especially in military application security is mandatory. Many security protocols have been proposed which mainly focus on the security issues related to data integrity, confidentiality and other focus on availability.

As MANETs is specifically designed for military application and disaster recovery operations, just resource reservation to achieve QoS is not enough but also robust against security threats. Hence the proposed research will mainly focus on Improving QoS in MANETs. The research will be carried out using analytical and mathematical modeling along with simulations. The research objective is to improvement of QoS in MANETs. The research objective is to develop a method to mitigate the Blackhole attack in MANETs in an efficient way. The proposed research will mainly focus

1. Improving the Network performance by mitigating Attacks
2. Secure communication by assuring trust
3. To develop a security mechanism to mitigate attacks.

This will improve overall scalability, throughput, transmission overhead and Security of mobile ad hoc networks. We have investigated research problem by creating a network of number of mobile nodes and transmit the data packets to each other and verify the simulation results with the help of appropriate simulation technique.

Black Hole Attack is a sort of negation of service attack. when a malicious node can attract all packets by false pretences a fresh route until destination, then soak up them without for-warding them to the destination and seggast to as a node dropping every packet and sending counterfeit routing packets to route packets over itself. The sink node (the destination) to attract additional traffic to the malicious node and then drops them [1]. Also implemented on the AODV protocol. Also find the malicious node. Based on the trust value of node& define which path is most suitable for routing the packet and untrusted node can easily remove or ignored [3]. Provide methods to detect malicious nodes but that is not sufficient to solve the black hole problem and the more detection method should be initiated to solve the black hole attack. [6] the traffic involving in a destination node, itsDst Seq may change. As the last in the black holeat-tack, the Specifically investigate the effects of the attack when the number of connections to the number of connection from the destination are changed. [8]

II. LITERATURE SURVEY

Ayesha Siddiqua et. Al (2015) proposed an approach for detection and prevention of Black hole attack using secure knowledge algorithm in which it used promiscuous mode to ensure data delivery to receiver node, also finds packet drop reasons before declaring node as a black hole node. In this method, AODV protocol is modified, so that every node in a network listens to its neighboring nodes promiscuously and nodes compares the neighbor node information stores in its fm and rm table entries: fm table hold the detail about recent packet forwarded. rm table hold the insight about neighboring hub detail like goal address, TTL esteem, and Node Energy. If any entries in the table which has fm ≠ rm and threshold value is reached, then modification attack otherwise trusted node. On the off chance that rm and edge esteem is achieved then Black opening assault.

Miss Bhandare A.S. et. Al (2015) proposed an approach against Co-operative Black hole attack in which it used detection and defense mechanism is proposed to remove the intruder that bring out black hole attack by taking decision about safe route on basis of Normal V/S Abnormal activity. Various Fake RREP Parameter like Destination Sequence Number, Hop Count, Destination IP Address, Time Stamp are considered are make them decision to identify the attack is called Malicious Node Detection System (MDS). This method improved the PDR up to 76 to 99 %. The advantage of this method is that decision about unsafe route is taken independently by source and no any additional overhead required.

Nidhi Choudhary et. Al (2015) proposed solution for avoidance of black hole attack by detection of the malicious attacker using timer based detection approach. In this method each node defines a trust value for its neighbor node and inserts a timer with each data packet, if the trust value decreases below a threshold value for any node then all other nodes put that node in their blacklist table.

Ali Dorri et. al. (2015) proposed solution for detection and elimination of cooperative Black Hole Attack, when the source node wants to send data packets to the destination, at first it uses AODV routing protocol to find a recent fresh path. By selecting the best path, the source node checks the Next_Hop_Node and Previous_Hop_Node of the RREP in order to check the safety of the path. By using a Data Routing Information table (which

has Node Id, From and Through column; Indicates receive data from the specific node and the node sent packet data through the specific node in the network respectively,) the source node can detect malicious nodes and eliminate them from the network. In this Proposed Method used TCP connections in order to decrease false positive detection. By Simulation results, it decreased the packet overhead and processing time in malicious nodes detection.

But still the detection of Black hole in ad hoc is considered as a challenging task. Ankita Joshi et al., [15] proposed a three dimensional check algorithm which performs security checks on the basis of three parameters that are acknowledgement received before time out for packets send, checking residual energy of nodes and finally verifying with digital signature. The proposed approach is tested for multi hope hybrid Ad-hoc networks

III. PROPOSED WORK

Every node in a network receives a public key infrastructure from trusted third party by securely using RSA algorithm. Black hole attack initiates the malicious activity by giving false route reply message. In order to get integrity of route replay message, destination node needs to replay the route reply by using proposed algorithm.

Algorithm

1. Destination get the RREQ packets from different node
2. Node selects a best route based on metric less hop count, and prepare the route replay packet
3. Node adds the route replay packet with its secrete key got from the PKI

$(RREP)$ XOR (Secrete Key)

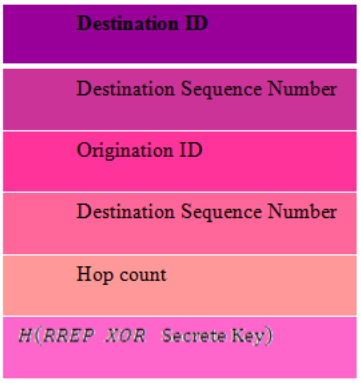
4. Node calculate the message digest using the digest algorithm according to PKI instruction (In our method it is MD5)

$H(RREP\ XOR$ Secrete Key)

5. Node append the calculated digest information with original route replay packet
6. RREP unicast towards the source node
7. Source node remove the $H(RREP\ XOR$ Secrete Key) from the RREP packet and adds the secrete key got from the PKI and perform the following task

$(RREP)$ XOR (Secrete Key)

$H(RREP\ XOR$ Secrete Key)



RREP Packet format of proposed protocol

And compare the calculated information with obtained information if both matches, then source node conclude that the information did not tamper during the communication

In our approach, every node in a network listens to its neighboring nodes promiscuously. In promiscuous mode, every node monitors the packet being forwarded by its neighbors in order to observe the behavior of neighbor regarding packet operation. Every node compares the neighbor information with the information it stores in its knowledge table. If both are same the node assumes that the packet is forwarded further, otherwise node waits for particular amount of time and checks the reasons for packet dropping. In order to confirm packets are sent to its neighbor, the nodes monitor the control packets as well as data packets to prevent selective dropping, as black hole attack drops selected packets. In order to monitor the forwarded packets, every node has to maintain knowledge tables with following entries: fm, rm if the values differ, the nodes are black hole nodes. If node does not forward the packet than the node at the instance checks the other reason for packet dropping, specified in our algorithm. If the packet dropping reaches to a threshold value, the node is identified as malicious node and is removed from route selection. It first checks, whether the next node is destination node or not, and also checks the TTL, if its same then it checks node properties such as residual energy(ce).

Knowledge table contains the information about the packet which is most recently transmitted. When any node detects a black hole node in a network, it broadcasts the node‟s id to other nodes so as that the malicious node can be avoided in routing process. Our algorithm is based on AODV, where the best path is based on minimum hop and maximum sequence number.

When source wants to send the information to destination, it broadcast the control packet RREQ to its entire neighboring node. RREP is generated by destination through trusted nodes only, if any node is found malicious during route discovery

process, its information is transmitted to all other nodes. If already a route is established and later it learns that one of the nodes of its route is a black hole node than the source node removes that node and re-initiates the routing process.

IV. RESULT AND DISCUSSION

4.1 Introduction

Multi-hop wireless ad hoc network composed of wireless mobile devices communicate by relaying on intermediate node. This network characterized by lack of infrastructure, without central coordinator and constrained resources. Routing is possible by assumption that nodes in a network are cooperative, but it is not always true in distributed constrained resource environment. Attacker can perform the malicious activities by not following routing protocol stipulations, one such attack is black hole attack. In which attacker node manipulate the control message and attract the communication information towards it and then drop the information. Prior work detects and remove the black hole attack by monitoring the nodes, which is not feasible solution in hostile environment. We mitigate the black hole attack by PKI. Simulation results shows that our proposed method accurately prevent the black hole attack and hence extend the network performance.

In this chapter, it describes experimental results and discussions on the simulated results. It also compares the performance of the algorithms in wireless network.

4.2 Screen Shots

A TCL file is used to create a network scenario which contains the information regarding topology size, number of nodes and configuration of nodes and packet information, energy model, node's initial energy, routing protocol, routing mechanism and traffic patterns to route the packets which generate trace files and NAM file. NAM file when executed visualize the simulation of network.

ns command is used to run TCL files which interacts with the interpreter and allows TCL procedure to be invoked at arbitrary points in simulation time.

The TCL files when executed generates the following NAM and trace files according to the protocol defined in it.

Using ns2, to calculate simulation with existing extension in ns2 libraries and compared our work with

- AODV without black hole attack.
- AODV with black hole node in network.
- Proposed algorithm/work with black hole node in network.

Below figures displays the trace file output according to proposed protocols displaying node energy, type of traffic, position of nodes etc. NAM is a TCL/TK based movement apparatus that is utilized to picture the ns reproductions and genuine bundle follow information. The first step to use NAM is to produce a nam trace file.

4.3 Performance Evaluation

To evaluate the performance the implemented protocols are compared with the existing protocols.The trace files generated is used and using awk scripts various parametric values are collected and graphs are plotted using XGRAPH.

Table 4.1 shows the simulation parameters set for the proposed protocols.

PARAMETERS	VALUES
Nodes	10-40
Channel	Wireless channel
MAC	802.11
Routing	AODV, Proposed(SAODV)
Querying	Priority queue
Simulation time	0.9
Network area	1000x1000 meters
Packet size	512
Traffic	CBR(constant bit rate)

Performance Analysis Metrics:

- **Packet Delivery Ratio(PDR):**

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

- **Throughput**:

Throughput is a measure of what number of units of data a structure can process in a given measure of time. It is applied broadly to systems ranging from various aspects of computer and network systems to organizations. Generally, it is the maximum rate of production or the maximum rate at which something can be processed.

- **Packet Overhead:**

The time it takes to transmit data on a packet-switched network. Each packet requires extra bytes of format information that is stored in the packet header, which, combined with the assembly and disassembly of packets, reduces the overall transmission speed of the raw data.

Delay:
System delay is an imperative plan and execution normal for a PC system or media communications arrange. The delay of a network specifies how long

it takes for a bit of data to travel across the network from one node or endpoint to another. It is commonly measured in products or parts of seconds. Delay may contrast slightly, contingent upon the area of the particular match of imparting nodes.

V.RESULTS

In this section we are analyzing our proposed work with the presence of malicious node in a routing path with varying number of nodes from 10 to 30 with respect to throughput packet loss and delay

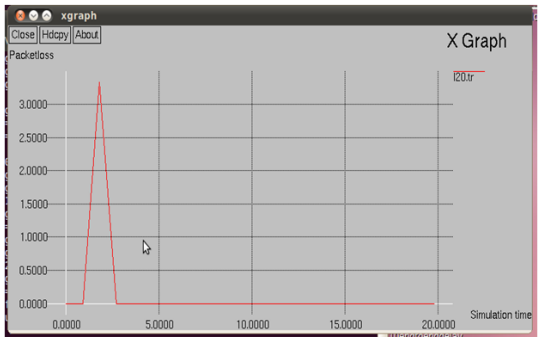


Figure4.1.Delay proposed work, number of node with malicious node

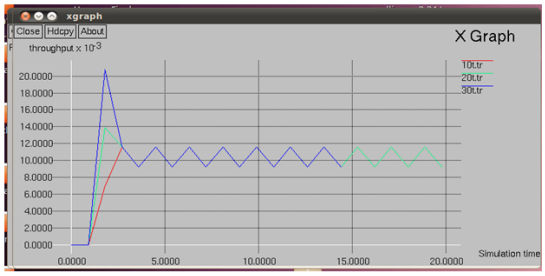


Figure4.2. Throughput comparison of number of node with malicious node

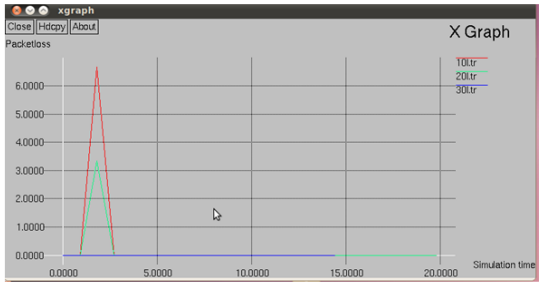


Figure4.3. Pack loss comparison of number of node with malicious node

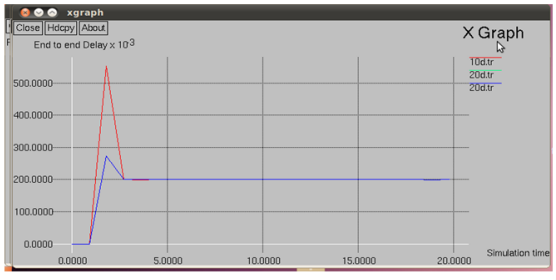


Figure4.4. End to End Delay comparison of number of node with malicious node

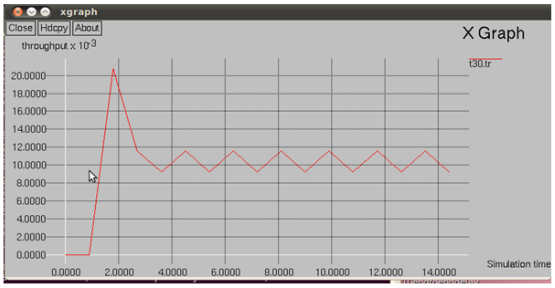


Figure4.5. Throughput of number of node (30) with malicious node proposed protocol

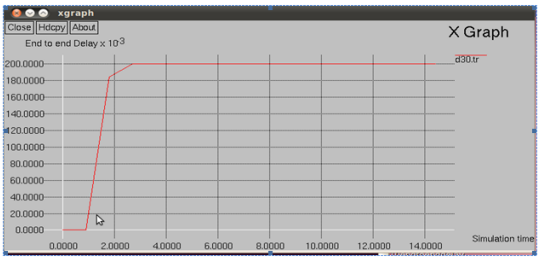


Figure 4.6. Delay of number of node (30) with malicious node proposed protocol

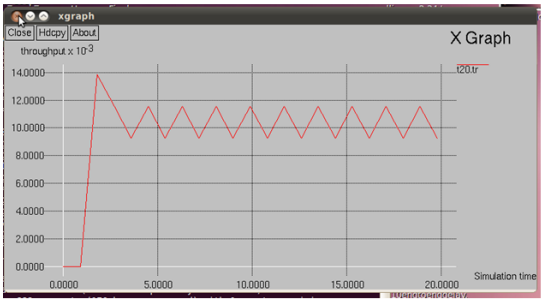


Figure 4.7. Throughput of number of node (20) with malicious node proposed protocol

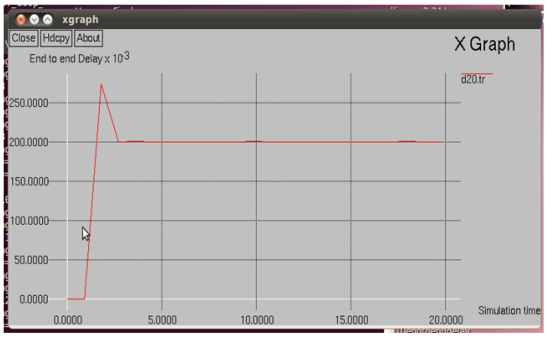


Figure 4.8. Delay of number of node (20) with malicious node proposed protocol

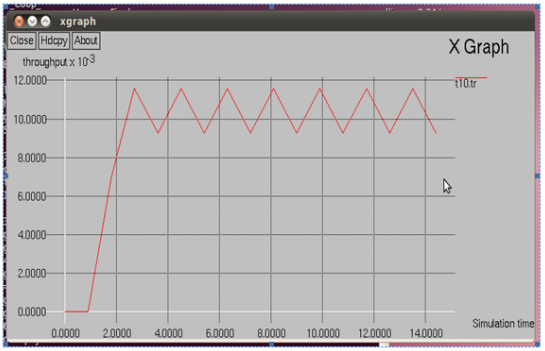


Figure 4.9. Throughput of number of node (10) with malicious node proposed protocol

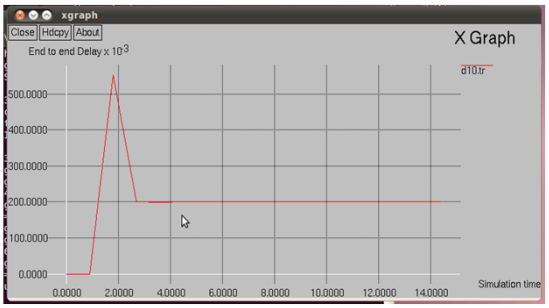


Figure 4.10. Delay of number of node (10) with malicious node proposed protocol

Performance comparison of proposed work is discussed in figure 4.1 to 4.10, it is clearly indicating that our proposed work mitigates the malicious attack from routing path and enhance the throughput with less delay and considerable overhead. In below section we are comparing our work with existing monitoring based proposed work to mitigate the black hole in mobile ad hoc networks, the comparison results are shown in below figures 4.11 to 4.16.

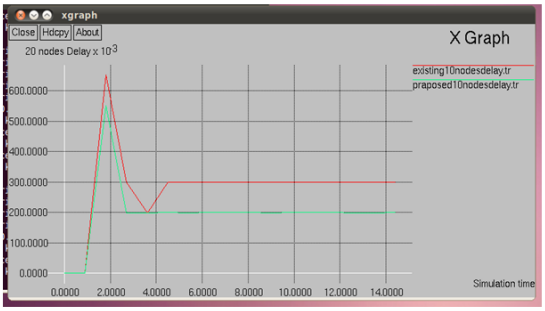


Figure4.11. Comparison of Delay of number of node (10) with malicious node proposed protocol with existing protocol

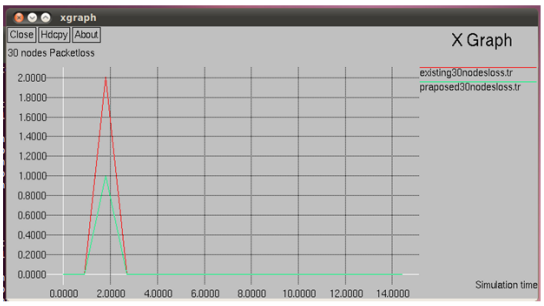


Figure4.12. Comparison of packet loss number of node (30) with malicious node proposed protocol with existing protocol

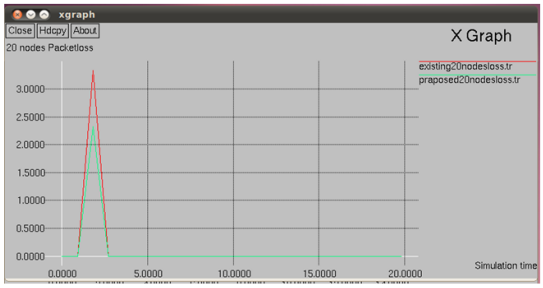


Figure4.13. Comparison of packet loss number of node (20) with malicious node proposed protocol with existing protocol

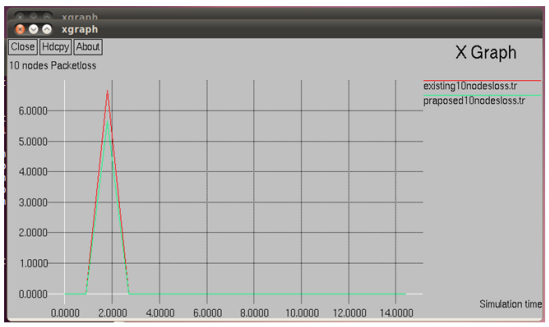


Figure 4.14. Comparison of packet loss number of node (10) with malicious node proposed protocol with existing protocol

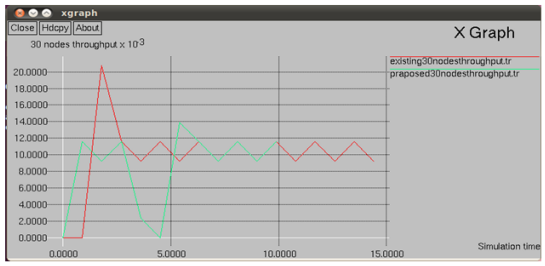


Figure4.15. Comparison of Throughput number of node (10) with malicious node proposed protocol with existing protocol

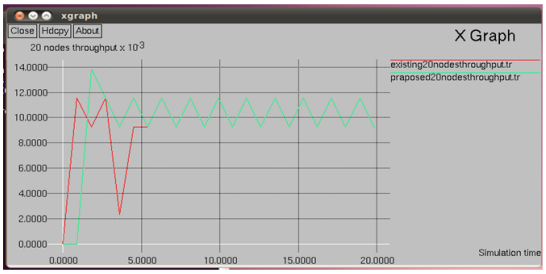


Figure4.16. Delay of number of node (20) with malicious node proposed protocol

Figure 4.11 to 4.16 compares the performance of existing protocol with proposed protocol with varying number of nodes from 10 to 30 with the presence of malicious node. However, results clearly indicate that our proposed work performed well in comparison with existing work. Thus we compare the proposed work and existing work in tabular form which is given below table 4.2

VI. CONCLUSION

In this project work a „PLI based algorithm" for mitigating black hole attack in AODV protocol has been proposed, which is used to provide security to the MANETs. This algorithm prevents the black hole attack at initial stage. The main goal of SKA is not only to mitigate black hole attack but also to increase the throughput thereby reducing the packet loss due to black hole node. If any node drops a packet our algorithm checks for the packet drop reasons first before declaring it as a black hole node, thereby preventing a trusted node from becoming a black hole node.

The main goal of SKA is not only to mitigate black hole attack but also to increase the throughput

thereby reducing the packet loss due to black hole node.

In future, we can work on Co-operative Black hole attack detection & prevention by using Cryptographic techniques.

VII. REFERENCES

[1] Surana K.A., rathi s.b., thosar t.p. and snehal mehatre, Securing black hole attack in routing protocol aodv in manet withwatchdog mechanisms, world research journal of computer architecture (2012)

[2] Dr. V Sankaranarayanan, prevention of co-operative black holeattackinmanet,journal of networks, 2008.

[3] Nirali Modi, Vinit Kumar Gupta, prevention of blackholeattackusingaodvroutingprotocol in manet, (ijcsit) international journal of computer science and information technologies, 2014.

[4] Piyush Khemariya, Upendra kumar Purohit** & Umeshbarahdiya,performance study of improved aodv against black hole attack in wireless environment, international journal of engineering research and modern education (ijerme)(2016)

[5] Madhuri Gupta, Krishna Kumar Joshi, an innovative approach to detect the gray-hole attack in aodv based manet, international journal of computer applications ,2013.

[6] Heta Changela, Amit Lathigara, algorithm to detect and overcome the black hole attack in manets, international journal of computer applications ,2015.

[7] Lalita Prajapati, Anurag Singh Tomar, detection of black hole attack with improved aodv protocol in manet,(ijirset) 2015.

[8] Satoshi Kurosawa, Abbas Jamalipour, detecting blackhole attack on aodv-based Mobile ad hoc networks by dynamic learning Method, international journal of network security, 2007

[9] Neeraj Saini, Lalit Garg, enhanced aodv routing protocol against black hole attack, international journal of advanced,2014.

[10] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks." Indian journal of science and technology 9, no. 26 (2016).

[11] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "energy aware routing for manets based on current processing state of nodes." journal of theoretical & applied information technology 91, no. 2 (2016).

[12] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "analytical model for evaluating the bottleneck node in manets." indian journal of science and technology 9, no. 31 (2016).

[13] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "preventing black hole attacks in manets using secure knowledge algorithm." in signal processing and communication engineering systems (spaces), 2015 international conference on, pp. 421-425. Ieee, 2015.

[14] Mohammad, Arshad Ahmad Khan, and c. Atheeq. "mutual authenticated key agreement scheme for integrated internet manets." (2016)

[15] Ankita Joshi, Er. Aditi Agrawal, Prof A. K. Jaiswal, Dr. Rajeev Paulus, TD-DEEDV: A Technique to prevent collaborative attacks using Clustering and DigitalSignature in Multi Hop Hybrid Adhoc Networks, *International* Journal of Advanced Research in Computer Engineering & Technology (IJARCET)2016

