SECURITY ENHANCEMENT OF AODV ROUTING PROTOCOL FOR MULTIPLE BLACK HOLE ATTACKS

Mudita [1], Mohinder Singh[2]
[1] M.Tech Student, [2] Assistant Professor,
Department of Computer Science & Engineering,
Maharishi Ved Vyas Engineering College, Jagadhri, Yamunanagar

ABSTRACT

Adhoc routing protocols are susceptible to to various attacks due to the unawareness of the security aspect during their designs. A black hole attack interrupts usual network functionality by guiding bogus routing info in route finding phase. In this, we implemented a solution to avoid the black hole and the multiple black hole attackers on the AODV routing protocol in MANETs.

Keywords: Mobile Adhoc Network, Network Simulator, Route Reply, Route Request, Packet Delivery Ratio

1. INTRODUCTION

A mobile Adhoc network (MANET) is an amassing of wireless mobile hubs which can communicate with each other without having fixed system infrastructure or any central base station. Since mobile hubs are not controlled by some other controlling component, they have unlimited mobility and availability to others. Routing and system management are done agreeably by each different nodes. On account of its dynamic nature MANET has greater security issues than standard systems. It Stands for "Mobile Adhoc Network." A MANET is a sort of specially appointed system that can change areas and configure itself on the fly. Since MANETS are portable, they utilize wireless connections with interface with different systems. This can be a standard Wi-Fi association, or another medium, for instance a cell or satellite transmission.

1.1 MANET v/s WLAN

MANETs are progressively made and kept up by the individual hubs comprising the network. They don't require a prior design for correspondence purposes and don't depend on a wired foundation; in an ad hoc system all correspondence happens through a wireless median.
MANET contains an exceptional subset of remote systems since they don't require the presence of acentralized message-passing gadget. Simple wireless systems require the presence of access points or static base stations, which are in responsible of directing messages to and from mobile hubs inside the predefined transmission area.
Adhoc networks, then again, don't require the presence of any device other than at least two Mobile Nodes willing to agreeably form a system. Rather than depending on a wired base station to arrange the stream of messages to every mobile hub, the individual mobile hubs shape their own particular system and forward parcels to and from each other. This mobile conduct enables a system to be immediately shaped even under the most adverse conditions.

2. RELATED WORK

Deng et al. [1] proposed an algorithm to counteract black opening assaults in impromptu systems. As per the calculation, any hub on accepting a RREP bundle, cross checks with the following bounce on the course to the goal from a substitute way.

S. Ramaswamy et al. [2] recommended an algorithm to keep the co-agent black gap attack in specially appointed system. This algorithm depends on a trust connection between the hubs, and subsequently it can't handle dim opening attack.

S.Banerjee et al. [3] proposed a algorithm for discovery and evacuation of Black/Gray Holes. As per their algorithm as opposed to sending the aggregate information activity without a moment's delay, they isolate it into little measured squares, with the expectation that the noxious hubs can be detected& evacuated in the middle of transmission.

P.Agarwal et al. [4] introduced a method of building up a spine system of solid hubs. With the help of the spine system of solid hubs, source and goal hubs complete a conclusion to end checking to decide whether every one of the information parcels achieved the goal. On the off chance that checking brings about a disappointment, at that point the spine organize starts a convention for identifying the pernicious hubs.

S.Indrasinghe et al. [5] talked about the idea of statefull approach of IP tends to portion in specially appointed systems. Author have utilized this idea of spine hubs and planned a algorithm that is significantly less complex.

Mansoor Mohsin et al. [6] portrayed a complete protocol for identification and expulsion of systems administration Black/Gray Holes in Mobile ad hoc networks (MANET), by remembering that various individuals with mobile phones may interface together to shape a substantial gathering. Later on they may part into littler gatherings. This progressively changing system topology of MANETs makes it helpless for an extensive variety of attack.

Poongothai et al. [7] exhibited protocol investigation the different execution measurements like packet loss, bundle conveyance proportion and normal end to end delay. It is watched that the impact on packet loss is much lower as contrast with impact on delay.

Bo Sun et al. [8] disclosed an agreeable instrument to handle the black opening issue. The system is agreeable in light of the fact that hubs in the protocol work helpfully together with the goal that they can dissect, identify conceivable various black opening hubs in a more dependable manner.

Satoshi Kurosawa et al. [9] looked at the strategy proposed by different creators as indicated by their presumptions and the comparing reproduction result in NS2 exhibits that our convention averts black opening as well as enhances execution.

Payal N. Raj et al. [10] proposed the strategy utilized the RREQ, RREP, PDR, and PMIR as measurements to ascertain the QoS of a connection and into expectation of attack. Their proposed conspire was executed by them on NS-3test bed.

Mohammad Al-Shurman et al. [11] talked about two conceivable arrangements. The first is to discover in excess of one course to the goal. The second is to misuse the bundle grouping number incorporated into any parcel header. PC reproduction demonstrates that contrasted with the first specially appointed on-request separate vector (AODV) directing plan, the second arrangement can check 75% to 98% of the course to the goal relying upon the respite times at least cost of the postponement in the systems.

Chang Wu Yu et al. [12] proposed a circulated and helpful system to handle the dark gap issue. The instrument is dispersed so it can fit with the impromptu idea of system, and hubs in the protocol work helpfully together so they can break down, identify, and dispose of conceivable numerous black gap hubs in a more solid manner. Reproduction comes about demonstrate that our technique accomplishes a high black hole identification rate and great bundle conveyance proportion, while the overhead is nearly lower as the system activity increments.

AnuBala et al. [13] The reproduction result of the black hole attack by the assistance of system test system (NS-2) demonstrate the packet loss, throughput, and end-to-end postpone with black gap and without black gap on AODV in MANET. We broke down that the packet loss increments in the system with a black gap hub. Author likewise watched that the throughput and end-to-end defer diminishes in the system with a black opening hub.

Amos J Paul et al. [14] Mobile Adhoc networks (MANET) are broadly utilized as a part of spots where there is practically zero foundation. Various individuals with cell phones may associate together to frame a vast gathering. Later on they may part into littler gatherings. This powerfully changing system topology of MANETs makes it helpless for a wide assortment of assault. In this paper, they propose a total protocol for discovery and evacuation of Black/Gray Holes**.**

Neelam Khemariya et al. [15] an effective approach for the location and evacuation of the Black opening assault in the Mobile Ad Hoc Networks (MANET) is portrayed in it. The algorithm is actualized on AODV protocol. The algorithm can identifies both the single Black opening assault and the Cooperative Black gap attack.

Suparna Biswas et al. [16] According to our proposition, assessment of trust of each hub in the system depends on parameters, for example, security of a hub characterized by its portability and respite time, remaining battery control and so forth. This trust of a hub shapes the premise of choice of the most solid course for transmission. The reproduction comes about exhibit that our answer gives great execution as far as throughput, secure directing, and productive asset use.

Ali Dorri et al. [17] in this approach source hub checks both Next_Hop_Nodes (NHN) and Pervious_Hop_ Nodes (PHN) of Route Reply generator so as to check the security of way. By methods for Data Routing Information (DRI) table every single pernicious hub disposed of from the system. Reenactment comes about demonstrate that our approach diminished the preparing time and bundle overhead in contrast and another work. Furthermore, our approach distinguishes every malignant hub in a way in each keep running with no phony positive location.

Neha Sharmaet al. [18] a strategy is being proposed for recognition of the black gap or pernicious hub. In this strategy, another methodology a sort of trap technique is included AODV protocol for the identification of pernicious hubs. At the point when a black gap hub is distinguished then a disturbing procedure is activated to make different hubs mindful of malignant hubs.

Houda Moudni et al. [19] it upgrades the security of the Ad-hoc On-request Distance Vector (AODV) directing convention to experience the black hole attack. Their answer evades the dark opening and the different black hole attack

3. PROPOSED WORK

The primary thought behind this strategy is to list out the set of malignant hubs locally at every node at whatever point they go about as a source node. As said in the Assumption our protocol utilizes the idea of Core Maintenance of the Allocation Table i.e., at whatever point another node joins the network, it sends a communicate message as a demand for IP address.
The backbone node on accepting this message randomly chooses one of the free IP addresses. The new node on accepting the allotted IP deliver sends an affirmation to the BBN. Presently since the portion is just under the control of the Back Bone Nodes (BBN) the dynamic pool of unused/limited IPs of the system anytime of time is known just to the BBN.

4. RESULTS AND DISCUSSION

4.1 Simulation Flow

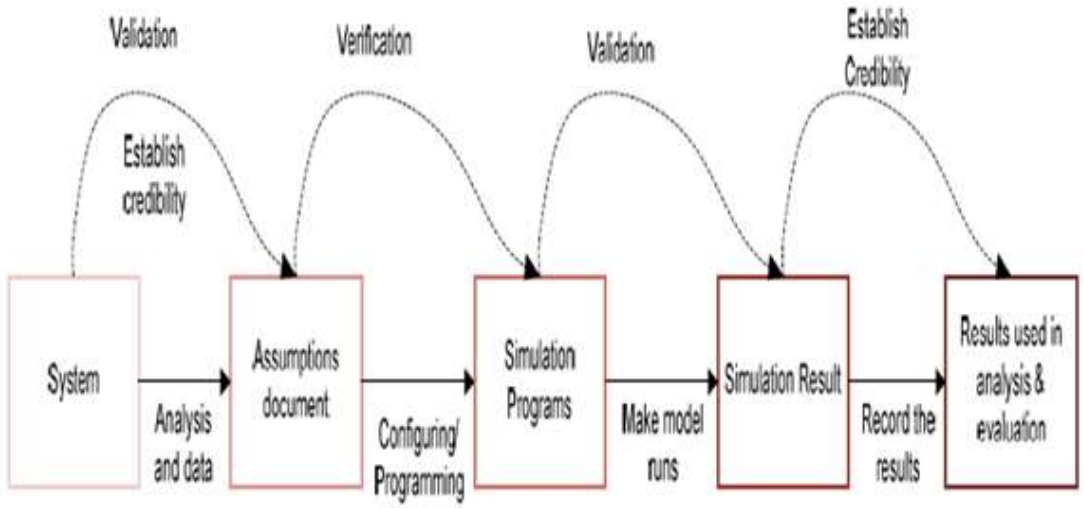

Figure 4.1 - A valid, credible and appropriate simulation model workflow

There are five states or steps of modeling the desired system represented by each rectangular box above. The horizontal arrows depict the actions to be taken in order to move from a state to another, while the bent dashed arrows represent where the validation, verification and credibility concepts are prominently established.

4.2 Simulation Model

Our simulation model was carried out utilizing the NS2 organize network simulator. In our work, we have attempted to assess the impacts of the Black Hole attacks in the wireless Ad-hoc Networks. To accomplish this we have reproduced the wireless ad-hoc network situations which incorporates Black Hole hub utilizing NS Network Simulator program. To simulate the Black Hole hub in a wireless ad-hoc network we have actualized another protocol that drops information packets subsequent to pulling in them to itself. In this part we present NS and our commitment to this software.

4.2.1 NS Network Simulator

NS is an event driven network simulator program, developed at the University of California Berkley, which includes many network objects such as protocols, applications and traffic source behavior. The NS is a branch of software of the VINT project that is supported by DARPA ever since 1995.

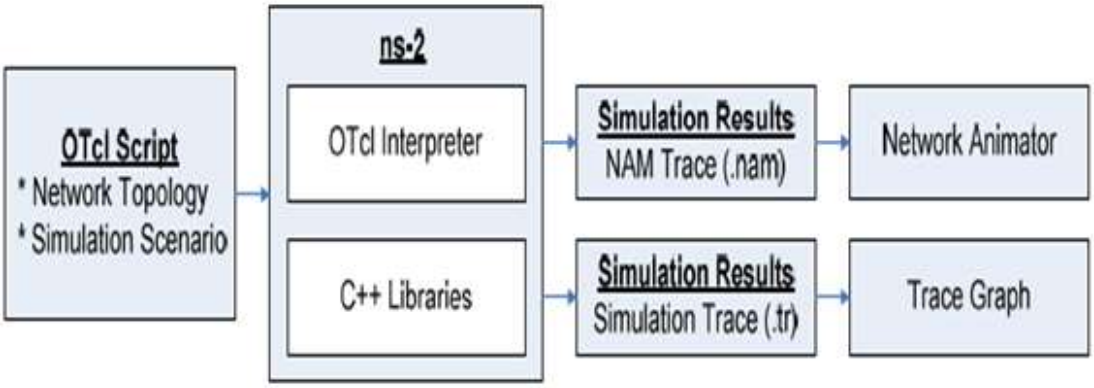

Figure 4.1 Components of Network Simulator

4.2.2 Evaluation of the Simulation

In the main scenario where there is certifiably not a Black Hole AODV Node, association between a some nodes being simulated is effectively imperfect when we take a animation of the simulation utilizing NAM. The output can be analyzed by watching the screen captures of the NS2 network simulator.

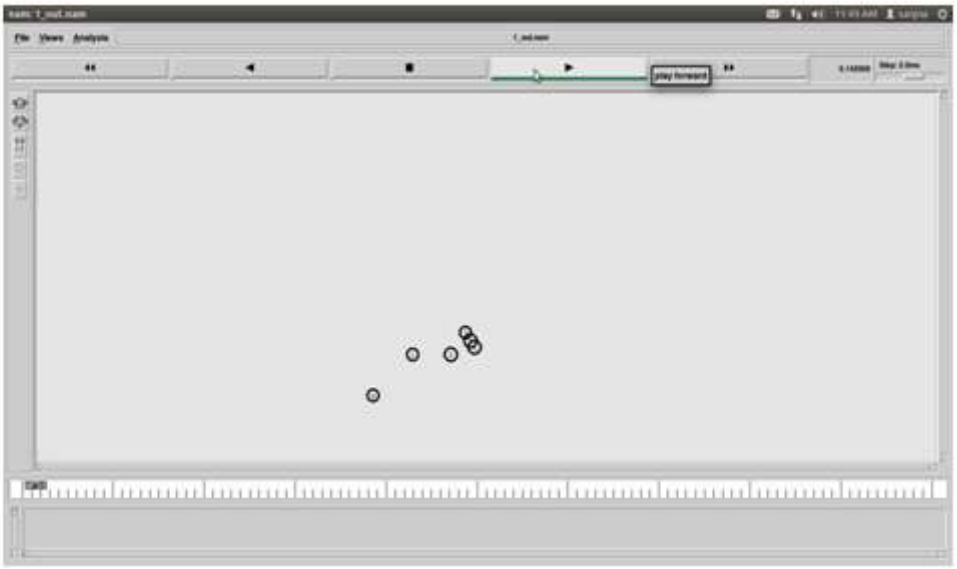

Figure 4.3

In the above figure 4.3 it is being observed that in the starting of simulation process one every node is working in cooperation with each other to keep the network in communication but as we proceed further there are situations in between where we have emergence of malicious node and the network resulted into the packet loss later on in the simulation process.

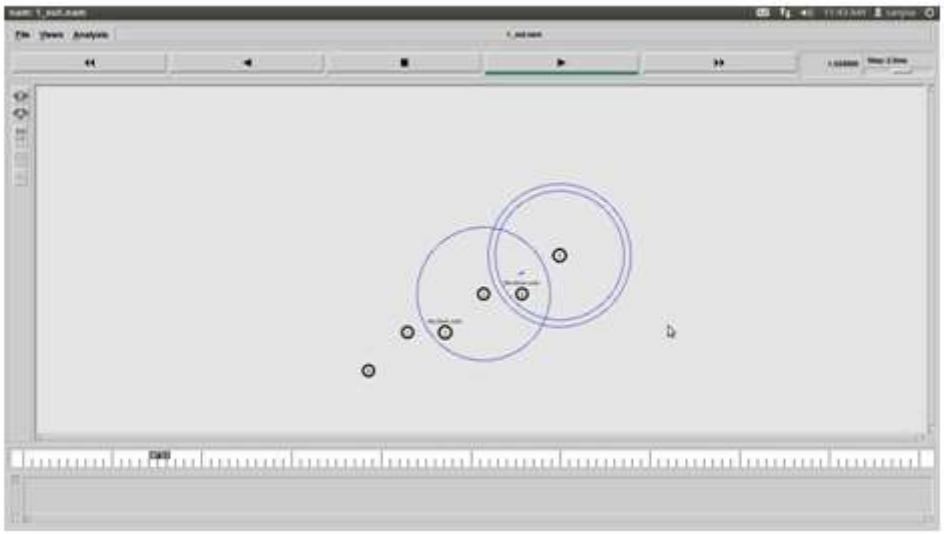

Figure 4.3.1

As shown in the above figure 4.3.1, the second simulation has one malicious node that carries out the Black Hole Attack. In our study, we try to compare the results of these two simulations to understand the network and node behaviors. We first try to evaluate the packet loss. Therefore we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes.

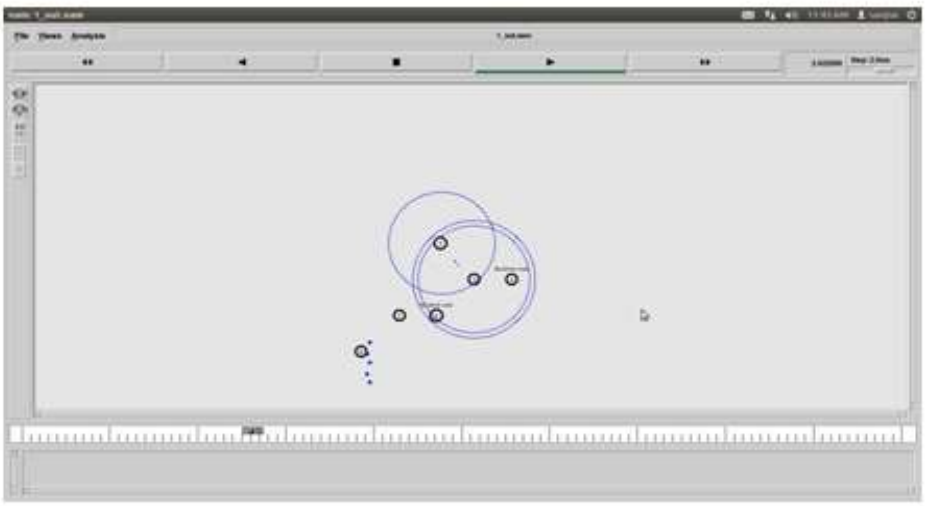

Figure 4.3.2

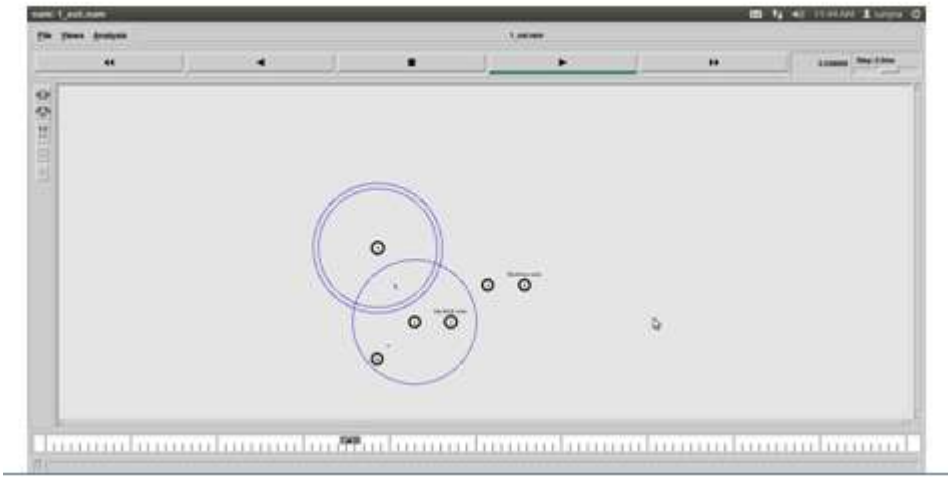

Figure 4.3.3

We first try to evaluate the packet loss in figure 4.3.2 and figure 4.3.3, then, we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes.

4.2.3 Analysis of Results

We have taken total of six nodes in our simulation evaluation process as shown in the figure 4.3 to figure 4.3.3 above. In the above figure it is being observed that in the starting of simulation process one every node is working in cooperation with each other to keep the network in communication but as we continue facilitate there are situations in the middle of where we have development of malicious node and the system came about into the packet loss later on in the simulation process. The second simulation has one malicious hub that does the Black Hole Attack. In our examination, we attempt to look at the aftereffects of these two simulations to comprehend the system and node behaviors. We first attempt to assess the packet loss. In this manner we tallied what numbers of parcels are sent by the sending hubs and what number of them achieved the accepting hubs. We endeavor to assess what number of the parcels which couldn't achieve the goal nodes are caught up operating at a profit Hole Node. We noticed that the percentage of data loss of the Black Hole AODV is increased more than the normal AODV network simulations in all situations. We also understand that the packet loss already exists in the network. This is because packets drop at the node interface queue due to the density of data traffic. To minimize the data traffic we alter node and packet parameters. Needing to evaluate the Black Hole effect in the network, we have to minimize the packet loss which happens at the network, except the Black Hole. In a wireless ad-hoc network which does not have any Black Hole, the data traffic might be dense and packets might get lost, for instance in a FTP traffic. Subsequently, the information loss does not generally say there was a Black Hole Node in the system. The whole scenario discussed above is displayed in figure 4.3 to figure 4.3.3, right from the foundation of the network displaying dynamic nature of the topology and at last displaying the data loss from the nodes due the commencement of the malicious node that is black node.

4.3.4 Graphical Result

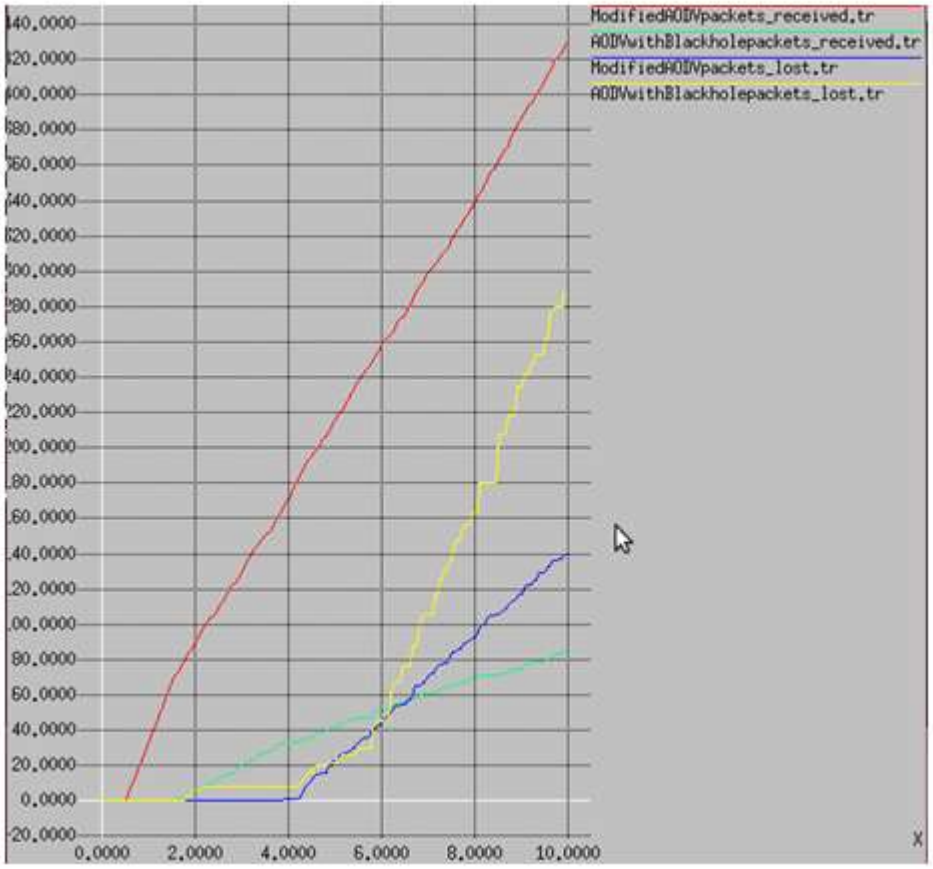

Figure 4.4(a) displaying the packet loss with respect to the time

In the above figure 4.4 (a) display the total packet received and total packet loss with both AODV with black hole and with AODV without black hole effect i.e. named as modified AODV in our approach. The total packet received without black hole in AODV (modified approach) is 420.000 where as the packet received in the AODV with introduction to black holes are 280.000. The modified approach consists of 120.000 packet loss where as the packet loss in AODV with black holes is 90.000 that are too low.

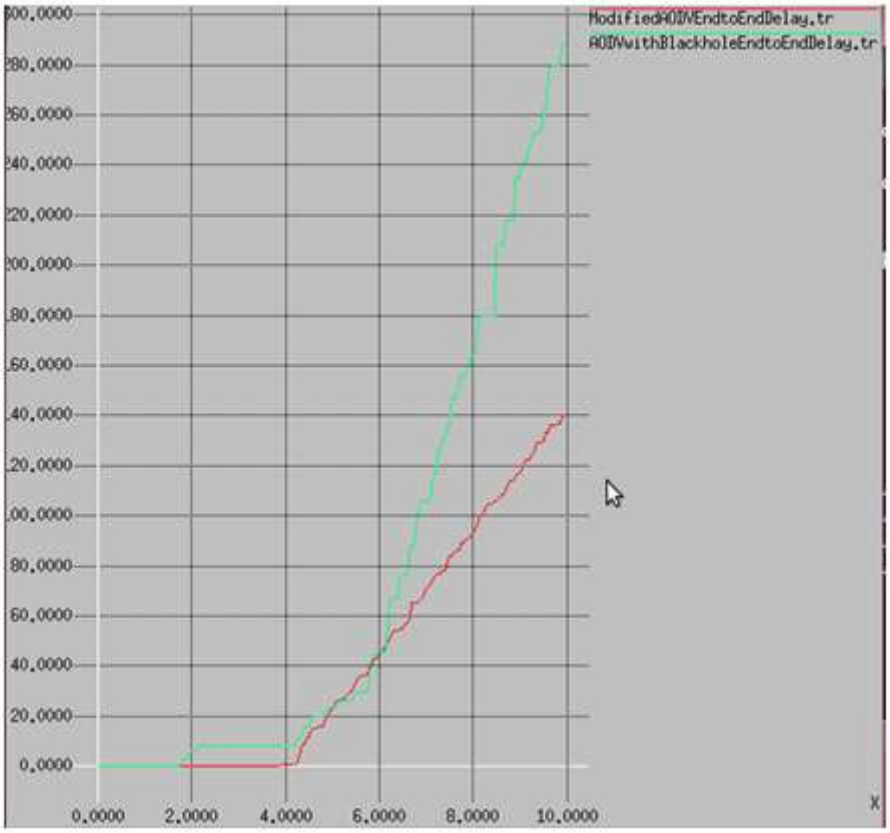

Figure 4.4(b) displaying the end-to-end delay with respect to the time.

In the above figure 4.4(b) displays the end-to-end delay with respect to time with both AODV with black hole is 290.000 and with AODV without black hole effect (modified one) is 140.00. The end-to-end delay in AODV with black holes is much more as compared to modified one i.e. the AODV without black holes.

5. CONCLUSION

Black hole and gray holes attacks are the most essential security issues in MANET. Black hole begins in route discovery stage and gray hole as an attack which drops bundles in transmitting step. Detection of gray hole is more troublesome than black hole, in light of the fact that the attacker works as normal node at that point begins dropping of data. In proposed work centers around identifying black and gray holes attacks, brought up their advantages and disadvantages and toward the end. Protection against both attacks in one detection system and diminishing number of errors is the primary intention. It is watched that the Black Hole impact the AODV protocol, likewise impact on packet loss is much lower as contrast with impact on delay. As malicious node is the primary security danger that impact the execution of the AODV routing protocol and their location is the fundamental matter of concern. Change for beating the impact of Black Hole should arrange towards controlling the postponement. In future this proposition is guided towards decrease the impact of Black Hole. The possible answer for recognize two sorts of malicious nodes (Black/Gray Hole) in the Adhoc network. The proposed arrangement can be connected to recognize and evacuate any number of Black Hole or Gray Hole Nodes in a MANET and find a safe way from source to goal by staying away from the over types of malicious nodes.

REFERENCES

[1] H. Deng ,W. Li and D.P. Agrawal , “Routing Security in Wireless Ad-hoc Networks”, *IEEE Communications Magazine,* pp.70–75, 2002.

[2] S.Ramaswamy, H. Fu, M. Sreekantaradhya , J.Dixon and K.Nygard, “Prevention of cooperative black hole attack in wireless ad hoc networks”, *Proceedings of the International Conference on Wireless Networks*.

[3] S.Banerjee , “Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks”, *In Proceedings of the World Congress on Engineering and Computer Science.*

[4] P. Agrawal, R.K. Ghosh and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", *Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication,* Suwon, Korea, pp. 310-314, 2008.

[5] Sudath Indrasinghe, Rubem Pereira and John Haggerty, "Conflict Free Address Allocation Mechanism for Mobile Ad Hoc Networks", *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW*), 2007.

[6] Mansoor Mohsin and Ravi Prakash, "IP Address Assignment in a mobile ad hoc network", *The University of Texas at Dallas Richardson, Mario Gerla Computer Science Department at UCLA,* Los Angeles, CA 90095.

[7] T. Poongothai and K.Jayarajan ,"A non-cooperative game approach for intrusion detection in Mobile Adhoc networks", *International Conference of Computing, Communication and Networking (ICCC),* St. Thomas, VI, pp 1-4, Dec 2008.

[8] Bo Sun,Yong Guan,Jian Chen and Udo , "Detecting Black-hole Attack in Mobile Ad Hoc Network", *The institute of Electrical Engineers, Printed and published by IEEE,* 2003.

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", *International Journal of Network Security*, Vol. 5, Number 3, pp 338–346, 2007

[10] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET", *International Journal of Computer Science Issues (IJCSI),* Volume 2, Number 3, pp 54-59, 2009.

[11] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", *ACM Southeast Regional Conference , Proceedings of the 42nd annual Southeast regional conference,* pp 96-97, 2004.

[12] Chang Wu Yu, Tung-Kuang, Wu, Rei Heng, Cheng and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", *International Workshop, Nanjing, China*, pp. 538–549, May 2007.

[13]. AnuBala, MunishBansal, Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009 IEEE.

[14]. Vishnu K, Amos J Paul, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications, 2010.

[15]. NeelamKhemariya, Ajay Khuntetha, "An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs", International Journal of Computer Applications, March 2013.

[16]. SuparnaBiswas, Tanumoy Nag, SarmisthaNeogy, "Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET", Applications and Innovations in Mobile Computing, 2014 IEEE.

[17]. Ali Dorri, HamedNikdel, "A New Approach for Detecting and Eliminating Cooperative Black hole Nodes in MANET", 7th International Conference on Information and Knowledge Technology, 2015 IEEE.

[18]. Neha Sharma, Annad Singh Bisen, "Detection As Well As Removal Of Black hole And Gray hole Attack In MANET", International Conference on Electrical, Electronics, and Optimization Techniques, 2016 IEEE.

[19]. HoudaMoudni, Mohamed Er-rouidi, HichamMouncif, Benachir El Hadadi, "Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack", 2016 IEEE