Comparison of AODV Protocol with the Revised AODV Protocol against Malicious Attacks

Clarita T. Pinto
Student of Dept. of C.S.E., M. Tech.,
Mangalore Institute of Technology and Engineering,
Mangalore, India.

Manjunatha A. S.
Asst. Professor, Dept. of C.S.E.,
Mangalore Institute of Technology and Engineering,
Mangalore, India

ABSTRACT
Mobile ad hoc networks (MANETs) are infrastructure less networks which consist of dynamic collection of nodes with rapidly changing topologies of wireless links. MANETS are mobile and therefore, they use wireless connections to connect to various networks. Devices in range can communicate in a point-to-point fashion. MANETs are liable to different types of DoS attacks in which packets are dropped. Black hole attack is an event that degrades the performance of the network.
This paper discusses the effects of the malicious attacks and the comparison of AODV Routing Protocol with the Revised AODV Routing Protocol in the presence of the Black hole attack based on performance metrics.

Keywords
MANET, Routing Protocols, AODV, Malicious attacks, Revised AODV

1. INTRODUCTION
A Mobile Ad-hoc Network **(**MANET**)** [1] is a self-configuring network of mobile routers (and associated hosts) connected by wireless links the union of which forms an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably.

These types of networks operate in the absence of any fixed infrastructure, which makes them easy to deploy, at the same time however, due to the absence of any fixed infrastructure, it becomes difficult to make use of the existing routing techniques for network services, and this poses a number of challenges in ensuring the security of the communication, something that is not easily done as many of the demands of network security conflict with the demands of mobile networks, mainly due to the nature of the mobile devices (e.g. low power consumption, low processing load).

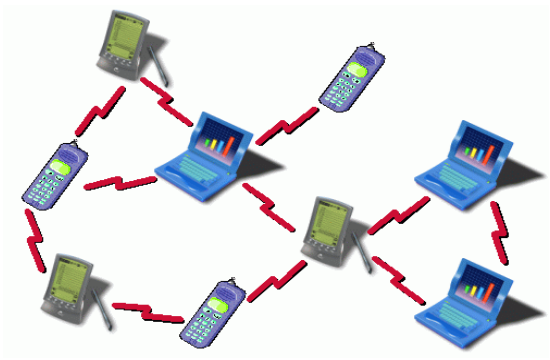

Figure 1: Mobile Ad hoc Network

1.1. Characteristics of MANET
1. In MANET, each node acts as both host and router. That is it is autonomous in behaviour.
2. Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
3. Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
4. The nodes can join or leave the network anytime, making the network topology dynamic in nature.
5. Mobile nodes are characterized with less memory, power and light weight features [2]

1.2. Applications of MANET
These are some of MANET applications [3]:

Table 1: MANET Applications

Application	Possible Scenarios / Services
Tactical Networks	• Military communications and operations • Automated battlefields
Emergency services	• Search and rescue operations • Disaster recovery • Replacement of fixed infrastructure in case of environmental disasters • Policing and fire fighting • Supporting doctors and nurses in hospitals
Home and enterprise networking	• Home/office wireless networking • Conferences, meeting rooms • Personal area networks (PAN), Personal networks (PN) • Networks at construction sites
Education	• Universities and campus settings • Virtual classrooms • Ad hoc communications during meetings or lectures
Sensor networks	• Home applications: smart sensors and actuators embedded in consumer

	electronics • Body area networks (BAN) • Data tracking of environmental conditions, animal movements, chemical/biological detection

1.3.Ad hoc Network Routing Protocols

Ad hoc network routing protocols [4] are categorized into three main categories:

1.3.1. Table Driven or Proactive Routing Protocol

1.3.2. On demand (demand driven) or Reactive Routing Protocol

1.3.3. Hybrid Routing Protocol

1.3.1. Table Driven or Proactive Routing Protocol

They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

Ex: Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR)

1.3.2. On demand (demand driven) or Reactive Routing Protocol

A different approach from table- driven routing is source-initiated on-demand routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a route discovery process within the network. This process is completed once a route is found or all possible route permutations have been examined.

Ex: Ad-hoc On Demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA).

1.3.3. Hybrid Routing Protocol

These protocols are both proactive and reactive protocols. These are designed to increase the scalability by allowing nodes with close proximity to work together to form some sort of backbone to reduce the route discovery overheads. This is achieved by proactively maintaining routes to nearby nodes and determining routes to far away nodes using a route discovery strategy. These protocols are zone based, which means that the network is partitioned as number of zones by each node.

Ex: Zone Routing Protocol (ZRP), Zone- based Hierarchical Link State (ZHLS)

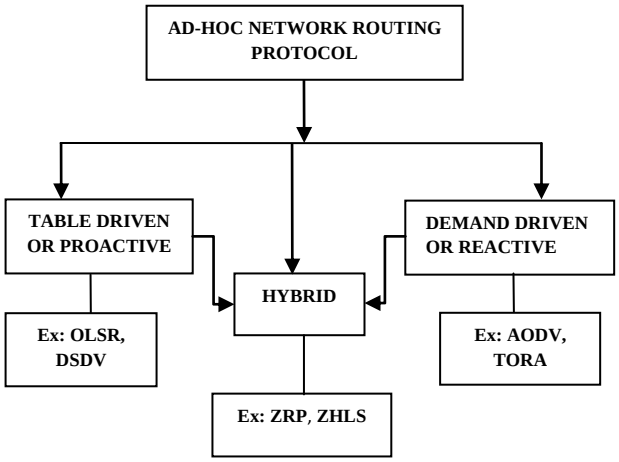

Figure 2: Ad hoc Routing Protocol classification

2. THEORETICAL BACKGROUND

2.1. AODV

Ad hoc On Demand Distance Vector (AODV) [5] is an On Demand Routing Protocol for wireless ad hoc networks. On demand algorithm, means that it builds routes between nodes only as desired by source nodes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. As the RREP propagates back to the source node, node's set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route.

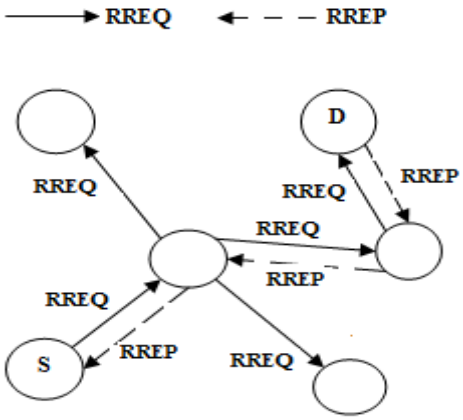

Figure 3: AODV Route Discovery Process

As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

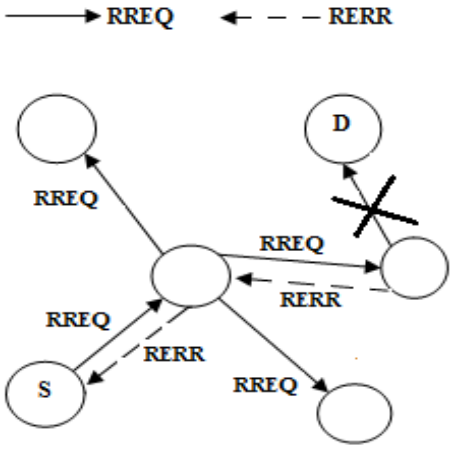

Figure 4: AODV Route Maintenance Process

2.2. Malicious Attacks

MANETs are liable to various types of malicious attacks such as Black hole attacks, sinkhole attacks, wormhole attacks etc. Black hole attack [6], which is Denial of Service (DoS) attack, is one in which a malicious node announces the freshest and shortest path to a destination node and then drops all data packets that subsequently goes through it.

The following figure illustrates the black hole attack. Malicious Node (Black Hole) announces itself as the shortest route to the destination and attracts all the data packets from the source node. Malicious node (Black Hole) drops all the data packets.

The effect of the black hole attack degrades the performance of the network because the destination node never receives the data packets as it is dropped by the malicious node.

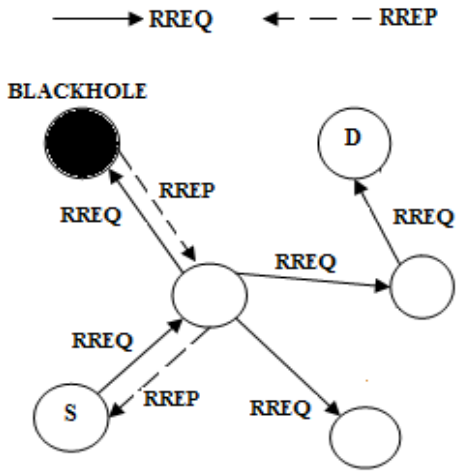

Figure 5: Black hole Attack

3. RELATED WORK

In order to make security of the network unbeatable, it is essential to develop security schemes that can take care of the malicious features of the nodes in Mobile Ad hoc Networks.

The authors in [7] have proposed to protect against the black hole attacks by waiting and checking the replies from all the neighboring nodes to find a safe route. Computer simulation using GLoMoSIM shows that SAODV protocol provides better performance than the conventional AODV in the presence of Black holes with minimal additional delay and overhead.

The study in [8], investigates the effects of Black Hole attacks on the network performance. They simulated black hole attacks in Network Simulator 2 (ns-2) and measured the packet loss in the network with and without a black hole. They also proposed IDSAODV against black hole attacks.

Enhanced AODV [9] (EAODV), the authors have proposed an improvement in the original AODV by introducing a new condition parameter for checking the RREP packet filter for better filtering mechanism.

The authors in [10] investigates some of the most severe attacks against MANETs namely the black hole attack, sinkhole attack, selfish node behavior, RREQ flood, hello flood, and selective forwarding attack. A detailed NS-2 implementation of launching these attacks successfully using Ad hoc On-Demand Distance Vector (AODV) routing protocol has been presented and a comprehensive and comparative analysis of these attacks is performed. They used packet efficiency, routing overhead, and throughput as the performance metrics.

The effects of Black Hole attacks on the network performance is analyzed using Qualnet Simulator has been proposed in [11] and measures the packet loss in the network with and without a Black Hole. The simulation was done on AODV (Ad hoc On Demand Distance Vector) Routing Protocol. The network performance in the presence of a Black Hole is reduced up to 26%.

The study in [12] analyzes the Black Hole attack which is one of the possible attacks in Ad hoc networks. They proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. They investigated the effects of the Black Hole attack in MANET using NS2 in their simulation. They have presented a new detection method based on dynamically updated training data.

4. REVISED AODV

This is the revised version of Ad hoc On Demand Routing Protocol (AODV) which is been incorporated with two new features: Multipath and Path accumulation.

In Multipath, the Revised AODV reduces the route discovery process as it finds multiple paths between the source nodes and destination nodes. It also reduces the number of similar routes between the source and destination nodes.

In Path Accumulation, the Revised AODV appends all the discovered routes between source and destination nodes to the control messages. Therefore, the RREQ packet at the intermediate node contains a list of all the nodes traversed.

The solution basically modifies the working of the source node, using an additional function called Pri_RREP(). A new table RREP_TAB, a timer WAIT_RREP_TIME, and a

variable MAL_NODE is introduced to the data structure in the existing AODV protocol.

In Revised AODV, all the route replies along with the destination sequence number and the node id are stored in the new table called RREP_TAB until WAIT_RREP_TIME time, which is initialized to half of the RREP_WAIT_TIME value. For WAIT_RREP_TIME time, the source node saves all the RREP's in the RREP_TAB table.

Then the source node examines all the stored RREP's in the RREP_TAB table and discards the RREP with the highest destination sequence number as it is the route reply which is obtained from the Black hole or malicious node.

Once the Malicious node is identified, then we call the ReceiveReply method of the existing AODV Routing Protocol.

The flowchart is as follows:

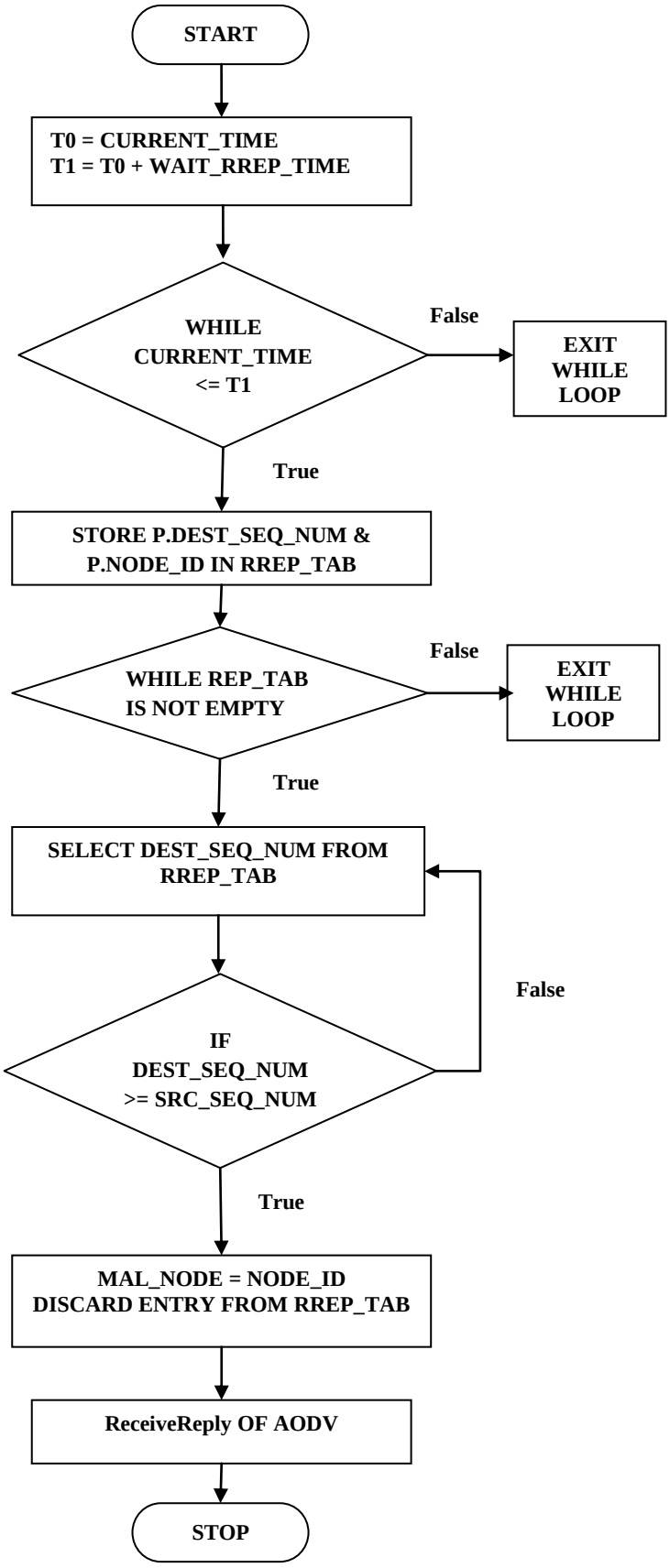

Figure 6: Flowchart of Revised AODV

5. EVALUATION METHODOLGY

5.1. Simulation Environment

5.1.1. Ns-2

NS or the network simulator [13] (also popularly called ns-2, in reference to its current generation) is a discrete event network simulator. NS is popularly used in the simulation of routing and multicast protocols, among others, and is heavily used in ad-hoc networking research.

NS2 supports an array of popular network protocols, offering simulation results for wired and wireless networks alike. Network simulator is an object oriented simulator.

At the physical and data link layer IEEE 802.11 is used. The channel used is Wireless Channel with Two Ray Ground radio propagation model. At the network layer, AODV is used as the routing protocol. UDP is used at the transport layer. The data packets are Constant Bit Rate (CBR) packets.

The mobility model is generated using the setdest utility. Setdest generates random positions of the nodes in the network with specified mobility and pause time.

Table 2: Simulation Parameters

Parameters	**Values**
Simulator	Ns-2.35 version
Data Packet Size	512 byte
Simulation Time	100 sec
Topology	1000 * 1000
Number of nodes	20
Pause Time	2 sec
Performance Metrics	Packet Delivery Fraction, End-to-End Delay, Normalized Routing Overhead
Number of malicious node	1
Traffic Type	Constant Bit Rate
Mobility	5-30 m/s
DoS Attack	Black Hole Attack
Routing Protocol	AODV, Revised AODV
Node Movement Model	Random Waypoint

5.2. Performance Metrics

5.2.1. Packet Delivery Fraction

The ratio of the number of delivered data packet to the destination is Packet Delivery Fraction. This illustrates the level of delivered data to the destination.

$$PDF = \frac{\sum Number\ of\ packets\ received}{\sum Number\ of\ packets\ sent}$$

5.2.2. End-to-End Delay

The average time taken by a data packet to arrive in the destination is called End-to-End Delay. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations are counted.

$$E-E\ Delay = \frac{\sum(Arrive\ Time - Sent\ Time)}{\sum Number\ of\ connections}$$

5.2.3. Normalized Routing Overhead

It is defined as the total number of routing packet transmitted per data packet. It is calculated by dividing the total number of routing packets sent (includes forwarded routing packets as well) by the total number of data packets received.

$$NRL = \frac{\sum Routing\ Packets}{\sum Received\ Packets}$$

5.3. Mobility Models

In the performance evaluation of a protocol for an ad hoc network, the protocol should be tested under realistic conditions including, but not limited to, a sensible transmission range, limited buffer space for storage of messages, representative data traffic models, and realistic movement of mobile users. This page describes several mobility models that represent mobile nodes whose movements are independent of each other [14].

Mobility models represent the movement of mobile users, and how their location, velocity and acceleration change over time. Such models are frequently used for simulation purposes when new communication or navigation techniques are investigated. [15]

Typical mobility models include [14] [15] [16] [17]:

5.3.1. Random Waypoint Model

5.3.2. Random Walk Model

5.3.3. Random Direction Model

5.3.4. Random Gauss-Markov Model

5.3.5. Manhattan Mobility Model.

5.3.1. Random Waypoint Model

The Random Waypoint Mobility Model [18] includes pause times between changes in direction and/or speed. A mobile node begins by staying in one location for a certain period of time (i.e., a pause time). Once this time expires, the mobile node chooses a random destination in the simulation area and a speed that is uniformly distributed between [minspeed, maxspeed]. The mobile node then travels towards the newly chosen destination at the selected speed. Upon arrival, the mobile node pauses for a specified time period before starting the process again.

6. RESULTS

6.1.Snapshots

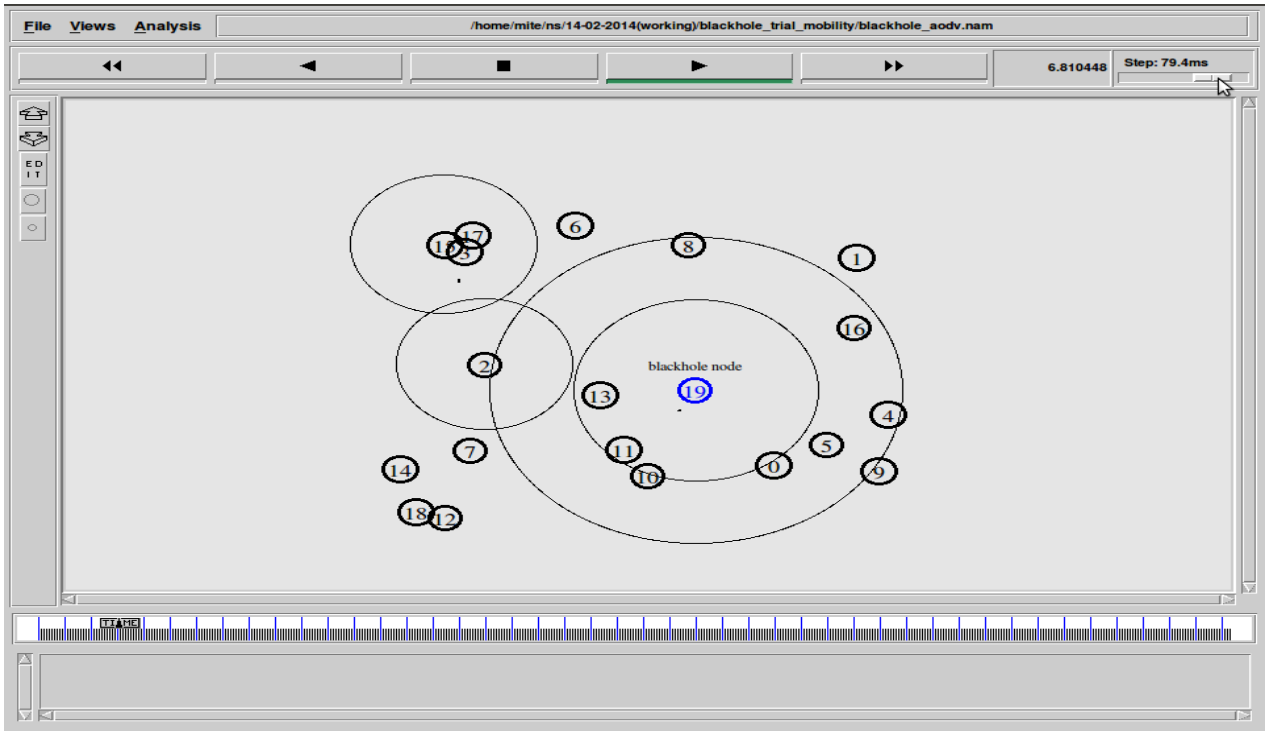

Figure 7: Network Scenario of Black hole attack in MANET

6.1.1. Packet Delivery Fraction

Figure 8: Impact of Black hole attack on Packet Delivery Fraction

The results of the simulation of Ad hoc On Demand Distance Vector and Revised AODV in the presence of Blackhole attack as shown in the figure 8, indicates the Packet Delivery Fraction in RAODV routing protocol increases compared to that of the AODV routing protocol.

6.1.2. End-to-End Delay

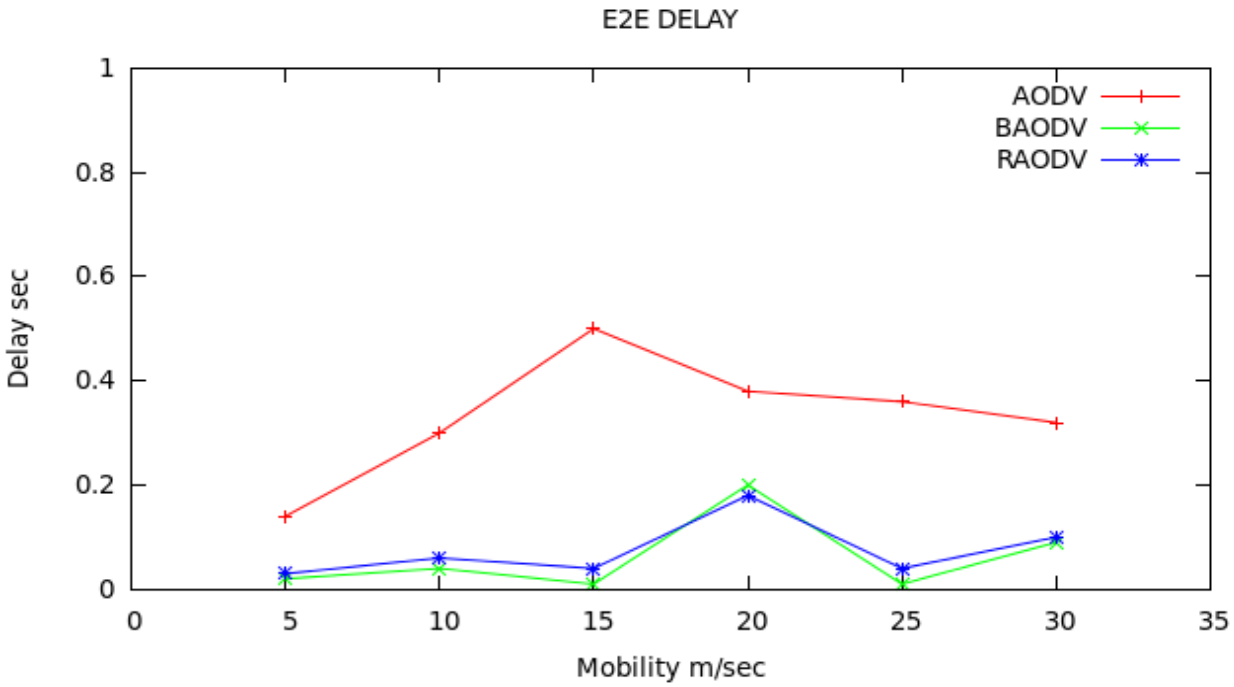

Figure 9: Impact of Black hole attack on End-to-End Delay

The results of simulation of Ad hoc On Demand Distance Vector and Revised AODV in the presence of Blackhole attack as shown in the figure 9, indicates the End-to-End Delay in RAODV routing protocol increases compared to that of the AODV routing protocol.

6.1.3. Normalized Routing Overhead

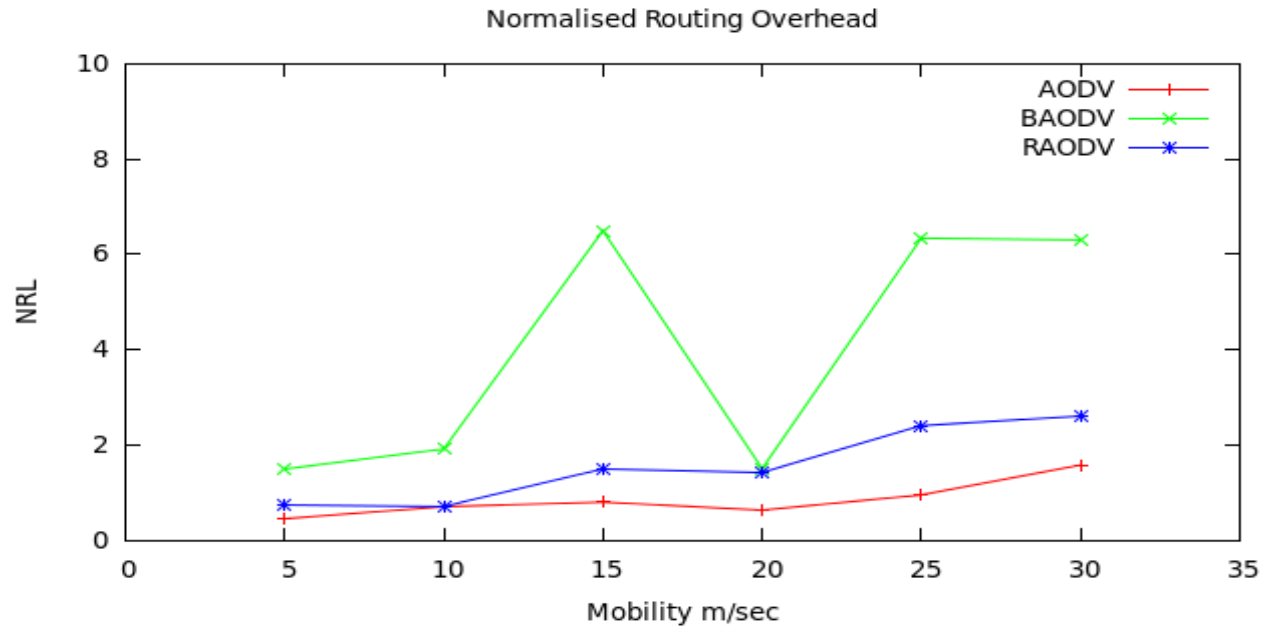

Figure 10: Impact of Black hole attack on Routing Overhead

The results of the simulation of Ad hoc On Demand Distance Vector and Revised AODV in the presence of Blackhole attack as shown in the figure 10, indicates the Normalized Routing Overhead in RAODV routing protocol decreases compared to that of the AODV routing protocol.

7. CONCLUSION

A Black Hole attack is one of the most serious security problems in MANET. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. This paper analyses the effects of malicious attacks such as black hole based on the performance metrics such as Packet delivery Ratio, End to End Delay, and Normalized Routing Overhead. It also analyses the liability of the two protocols AODV and Revised AODV by varying the mobility (speed). Simulation parameters used are important for evaluating the performance of the MANET Routing Protocol. The performance metrics such as Packet Delivery Ratio, End to End Delay and Normalized Routing Overhead are used as the measuring features.

8. REFERENCES

[1] MANETDefinition: http://www.techopedia.com/definition/5532/mobile-ad-hoc-network-manet.

[2] MANET Characteristics: http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, An Overview of Mobile Ad Hoc Networks: Applications and Challenges.

[4] M. Abolhasan, T. Wysocki, E. Dutkiewicz, "A Review of Routing Protocols for Mobile Ad- Hoc Networks", Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[5] C. E. Perkins, E. M. Belding Royer; and S. R. Das (2003) Ad hoc on demand distance vector (AODV) routing RFC 3561. The Internet Engineering Task force, Network Working Group.

[6] Ochola EO, Eloff MM, A Review of Black Hole Attack on AODV Routing in MANET.

[7] Tamilselvan, L. and Sankaranarayanan, V., "Prevention of Black hole attack in MANET". The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 21-21, 2007

[8] Dokurer, S.; Ert, Y.M.; and Acar, C.E., "Performance analysis of ad hoc networks under Black hole attacks", Southeast Con, 2007, Proceedings IEEE, 148 – 153.

[9] Black hole effect mitigations method in AODV routing protocol, 2011 IEEE, Zaid Ahmad, Kamarularifin Abd, Jamalul-lail Ab Manan.

[10] Humaira Ehsan, Farrukh Aslam Khan, "Malicious AODV-Implementation and Analysis of Routing Attacks in MANETs"- 2012 IEEE.

[11] Sheenu Sharma, Dr. Roopam Gupta, "Simulation Study of Black Hole Attack in the Mobile Ad hoc Networks", November 2009

[12] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Black hole Attack on AODV based Mobile Ad-hoc networks by Dynamic Learning Method. International Journal of Network Security", Vol.5, No.3, PP.338– 346, Nov. 2007

[13] ns-2, Network Simulator, http://www.isi.edu/nsnam/ns.

[14] Mobility Models: http://www-public.it-sudparis.eu/~gauthier/MobilityModel/mobility model.html

[15] Mobility Models: http://en.wikipedia.org/wiki/Mobility_model.

[16] Yogesh Chaba, R. B. Patel, Rajesh Gargi, "Analysis Of Mobility Models For Mobile Ad Hoc Networks" Voyager- The Journal of Computer Science and Information Technology, ISSN 0973-4872, Vol. 6, No. 1, July-Dec. 2007 p.p. 50-55.

[17] Bhavyesh Divecha1, Ajith Abraham, Crina Grosan and Sugata Sanyal, "Impact of Node Mobility on MANET Routing Protocols Models" School of Technology and Computer Science, Tata Institute of Fundamental Research, India.

[18] Tracy Camp, Jeff Boleng and Vanessa Davies, A survey of Mobility Models for Ad hoc Network Research, Wireless Communications and Mobile computing: A special issue on Ad hoc network Research, vol 2, No5, pp. 483-502, 2002.

[19] Modified AODV Protocol against Blackhole Attacks in MANET K. Lakshmi1, S.Manju Priya A.Jeevarathinam3 K.Rama4, K. Thilagam, International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.