INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 2151 Cities in 155 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the area of Computer, Business, Finance, Marketing, Human Resource Management, General Management, Banking, Insurance, Corporate Governance and emerging paradigms in allied subjects like Accounting Education; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Monetary Policy; Portfolio & Security Analysis; Public Policy Economics; Real Estate; Regional Economics; Tax Accounting; Advertising & Promotion Management; Business Education; Management Information Systems (MIS); Business Law, Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labor Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; Public Administration; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism, Hospitality & Leisure; Transportation/Physical Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Digital Logic; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Multimedia; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic and Web Design. The above mentioned tracks are only indicative, and not exhaustive.

Anybody can submit the soft copy of his/her manuscript **anytime** in M.S. Word format after preparing the same as per our submission guidelines duly available on our website under the heading guidelines for submission, at the email address: infoijrcm@gmail.com.

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF .**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mention the following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES & TABLES:** These should be simple, crystal clear, centered, separately numbered &self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, KurukshetraUniversity, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

PERFORMANCE ANALYSIS OF AODV PROTOCOL UNDER BLACK HOLE ATTACK

MONIKA SINGH
SCHOLAR
DEPARTMENT OF COMPUTER ENGINEERING
KAMLA NEHRU INSTITUTE OF TECHNOLOGY
SULTANPUR

RAKESH KUMAR SINGH
ASSOCIATE PROFESSOR
DEPARTMENT OF COMPUTER ENGINEERING
KAMLA NEHRU INSTITUTE OF TECHNOLOGY
SULTANPUR

ABSTRACT

A mobile ad hoc network (MANET) is an autonomous network that consists of mobile nodes that communicate with each other over wireless links. In the absence of a fixed infrastructure, nodes have to cooperate in order to provide the necessary network functionality. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc on demand Distance Vector) protocol.. The black hole problem is one of the security attacks that occur in mobile ad hoc networks (MANETs). In this paper we analyze the effect of black hole attack on AODV routing protocol under the light of various parameters such as packet loss, throughput, and end-to-end delay with black hole and without black hole on AODV in MANET. Here NS2 simulator is used for the simulation. The simulation result shows that the packet loss increases with the increase in the number of black hole node.

KEYWORDS

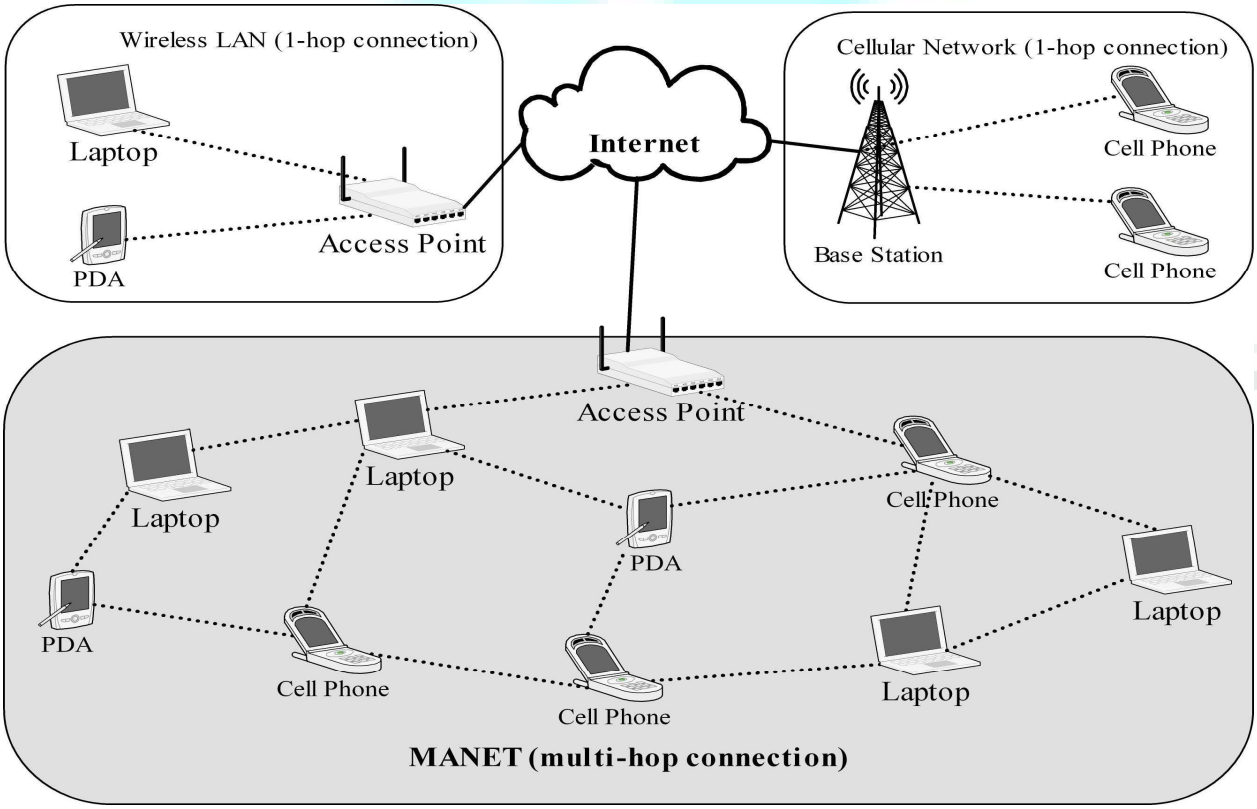
MANET, AODV, Black hole.

1. INTRODUCTION

Mobile Ad Hoc Networks [5] are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at same time. They can form arbitrary topologies depending on their connectivity with each other in the network.

MANETs must have a secure way for transmission and communication and this is quite challenging and vital issue as there is increasing threats of attack on the Mobile Network. In order to provide secure communication and transmission engineer must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

FIGURE 1: MOBILE AD-HOC NETWORK



Several technique exist to deal with the security issue in MANET .Previously the works done on security issues i.e. attacks (Dos attack) involved in MANET were based on proactive routing protocol like OLSR and its effects are elaborated by stating how these attacks disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET on the reactive protocol like AODV [2][4]. Thus our aim is to:

1 The study focus on analysis of Black Hole attack in MANET.
2 Analyzing the effects of Black Hole attack in the light of packet delivery ratio (PDR), number of packet lost and the network throughput in MANET.
3 Simulating the Black Hole attack using NS-2.34 for AODV Protocol.

This paper is organized as follows section 2 describe the black hole problem in manet after that in section 3 we had discussed some of the previous research work in this field. Section4 provides the various performance metrics used in our simulation and in section 5 we had provided our simulation work on AODV protocol using NS-2 simulator and finally section 6 conclude the whole research work followed by some of the future scope in section 7.

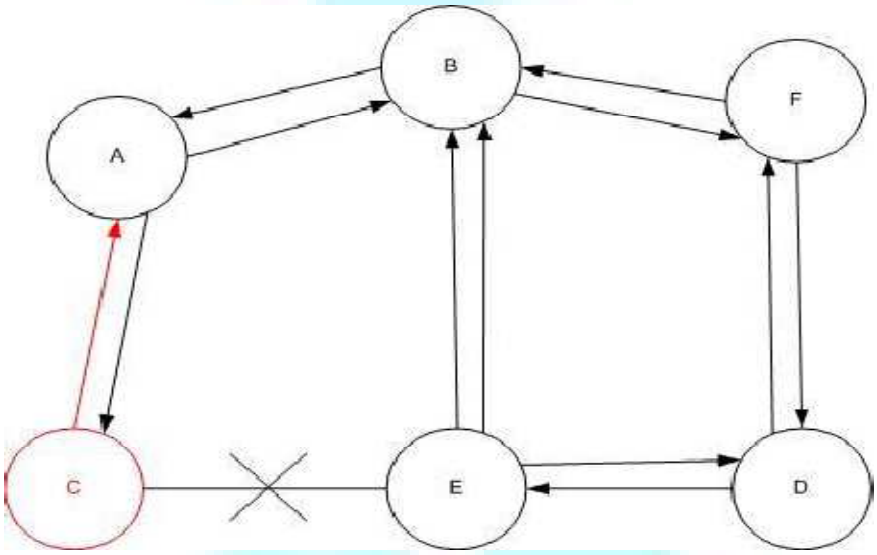
2. BLACK HOLE ATTACK

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept.

This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [8]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [3].

The method how malicious node fits in the data routes varies. Figure 2 shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

FIGURE 2: BLACK HOLE PROBLEM



3. LITERATURE REVIEW

Several researchers have studied the vulnerabilities of MANETs and black hole attack in particular. Black hole attack is one of the active DoS. Many researchers have proposed their solutions which are available in literature.

Mohd Al-Shurman *etal* [12] proposed two solution to overcome the problem of black hole.The first proposed solution for black hole is to find more than one route to the destination (redundant routes, at least three different routes). Then, the source node unicasts a *ping* packet to the destination using these three routes (we should assign different packet IDs and sequence number, so any node who receive the first packet will not drop the second one if it exists in both paths). The receiver and the malicious in addition to any intermediate node might have a route to the destination will reply to this ping request. The source will check those acknowledgements, and process them in order to Figure out which one is not safe and might have the malicious node. The second proposed solution exploits the packet sequence number included in any packet header. The node in this situation needs to have two extra tables; the first table consists of the sequence numbers of the last packet sent to the every node in the network, and the second table for the sequence number received from every sender. During the RREP phase, the intermediate or the destination node must include the sequence number of last packet received from the source that initiates RREQ. Once the source receives this RREP, it will extract the last sequence number and then compare it with the value saved in its table. If it matches the transmission will take place. If not, this replied node is a malicious node, so an alarm message will be broadcast to warn the network about this node. **Computer simulation shows that compared to the original *ad hoc on-demand distance vector* (AODV) routing scheme, the second solution can verify 75% to 98% of the route to the destination depending on the pause times at a minimum cost of the delay in the networks.**

The solution proposed in[9] require that the requesting node should wait for a predetermined set time to receive RREPs with next hop details instead of from other neighboring node sending data packets immediately after receiving a reply. After the time out, it first checks in CRRT table whether there is any repeated next hop node. If any next hop. node is present in the reply path it assumes the path is correct or the chance of malicious path is limited .Extra overhead is added in the process of finding repeated next hop and adds a delay.

In [3], the author proposed route confirmation request message (CREQ) and route confirmation reply (CREP) in order to avoid Black Hole attack. In this proposal when intermediate sends RREPs to the source node its send CREQ to its next hop node in direction of destination node. After receiving CREQ, the next hop look for route in its destination in cache. If its receive CREP during this time it will confirm the validity of path in RREP and in CREP. Upon matching the source node will recognize the route being correct. Its drawback is that it cannot detect multiple Black Hole attacks.

The protocol implement in [14] propose Secure Ad-Hoc On-Demand Distance Vector Routing (SAODV) which verify the destination node by exchanging random numbers. SAODV can effectively prevent Black Hole attack in Mobile Ad-hoc network and maintain better routing efficiency. It is better than AODV in terms of security and routing efficiency.

In [13], the author showed that malicious node should increase the sequence number of destination to assure the source node of its route. The author proposed a statistics based detection for Black Hole which is based on the difference between destination sequence numbers of received RREP's. Its drawback is the false positives approach because of the nature of anomaly detection.

The solution proposed in [10] focus on the requirement of a source node to wait unless the arrival of RREP packet from more than two nodes. When it receives multiple RREPs the source node check that there is any share hops or not. The source node will consider the routed safe if it finds the share hops. Its drawback is the introduction of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of node

In[11] author consider the limitations (battery power, storage and processing power) of nomadic computing paradigm, and devise an algorithm that prevents from black hole attack at the cost of only marginal processing overhead. The proposed algorithm is simple and does not affect workings of either intermediate or destination node. It does not even modify the working of normal AODV but calls a pre process called Pre_Process_RREP. The Process continues to accepts RREP packets and calls a process called Compare_Pkts(packet p1, packet p2) which actually compares the destination sequence number of two packets and selects the packet with higher destination sequence number if the difference between two numbers are not significantly high. Packet containing exceptionally high destination sequence number is suspected to be a malicious node and an ALERT message containing the node identification is generated which is broadcasted to neighbour nodes so that any message receive from such malicious node is discarded. A list of such malicious nodes can be maintained by the nodes participating in communication which can be used to prevent black hole attack

4. PERFORMANCE METRICS

This chapter focuses on result and its analysis based on the simulation performed in ns-2. Our simulated results are provided in Figures (6.1-6.9) gives the variation in network nodes while under Black Hole attack. To evaluate the behaviour of simulated intrusion based black hole attack, we considered the performance metrics of packet loss, throughput and packet delivery ratio.

4.1 PACKET LOSS

Mobility-related packet loss may occur at both the network layer and the MAC layer. Here packet loss concentrates for network layer. When a packet arrives at the network layer the routing protocol forwards the packet if a valid route to the destination is known. Otherwise, the packet is buffered until a route is available. A packet is dropped in two cases: the buffer is full when the packet needs to be buffered and the time that the packet has been buffered exceeds the limit.

PACKET LOSS =DATA AGENT SENT-DATA AGENT RECEIVE Equation 1

4.2 PACKET DELIVERY RATIO

The ratio between the number of packets originated by the “application layer” CBR sources and the number of packets received by the CBR sink at the final destination.

PDR=(∑CBR packets received by all sinks / ∑ CBR packet sent by all source) Equation 2

4.3 THROUGHPUT

It is the ratio of total amount of data which reaches the receiver from the sender to the time it takes for the receiver to receive the last packet. It is represented in bits per second or packets per seconds. In MANETs throughput is affected by various changes in topology, limited bandwidth and limited power. Unreliable communication is also one of the factors which adversely affect the throughput parameter.

5. SIMULATION RESULT

To calculate network performance, we simulate black hole node behaviour in AODV in large number of nodes and connections with the help of Network Simulator 2 [15] [6]. We set the parameters for our simulation as shown in Table 6.1. Xgraph [7] is used for plotting the result in form of graph in NS2[16]. The simulation parameters are shown below [1].

TABLE 1: SIMULATION PARAMETER

Simulator	NS-2.34
Simulation time	10sec
Number of nodes	40
Number of blackhole node	1
Topology	750m x 750
Routing Protocol	AODV
Traffic	Constant Bit Rate (CBR)
Maximum Connection	9
Packet size	512

In this section we present a set of simulation experiments to evaluate the effect of black hole attack on AODV protocol in MANET. First we had explained black hole attack in detail via simulation in NS-2.We have generated a small size network with40 nodes in a flat grid of 750m x750m including black hole node. We have generated 9 connections between various nodes. We have also introduced some movements in our scenario. duration of the scenario is 10 seconds. Node 25 is the source node, node 38 is the destination node and node 36 is the black hole node.

Figure 5.1 shows the snapshot of initially network. The route discovery process is shown in the Figure 5.2 for some seconds, the link breaks and all data that send from source node get lost as shown in Figure5.3. Now Figure.5.4 shows that node 36 starts acting as black hole node. Nodes further rebroadcast the request if they are not the destination nodes. Node 36 i.e. black hole node, claims that it has the route to destination whenever it receives RREQ packets and sends the response to source node. All other nodes that have the fresh route also send a reply. But the reply from node 36 reaches the source node first. Node 25 accepts it and ignores all other reply messages and begins to send data packets to node 38 via black hole node and node 36 being a black hole node absorbs all the packets and then instead of forwarding the packets to the destination it start dropping it and thus the packet will never reached its intended destination. This was shown in Figure 5.5.

FIGURE 5.1: INITIALLY NETWORK OF 40 NODES

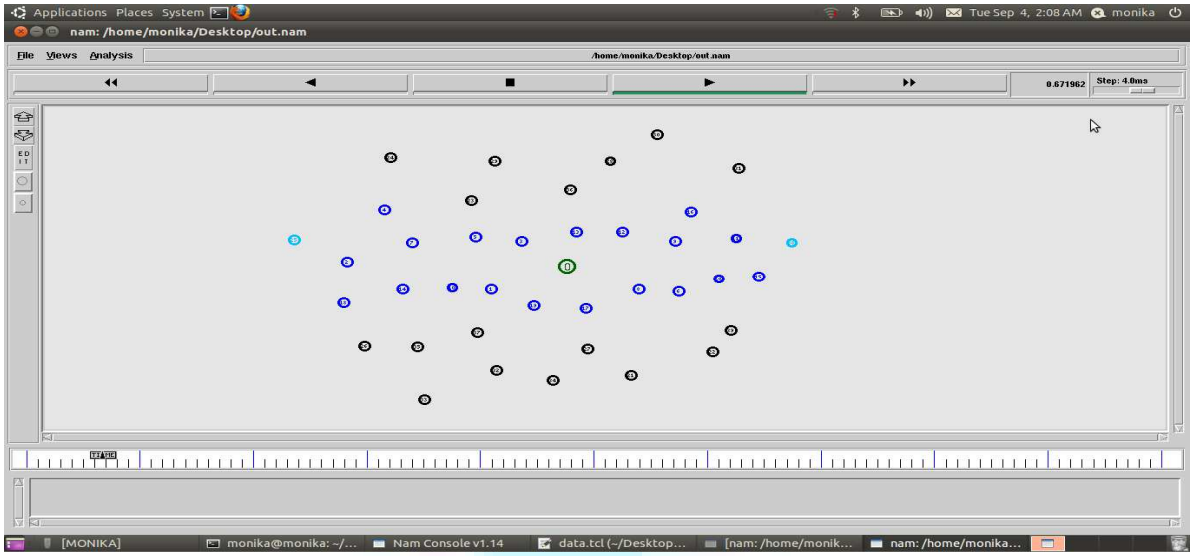


FIGURE 5.2: ROUTE DISCOVERY PROCESS

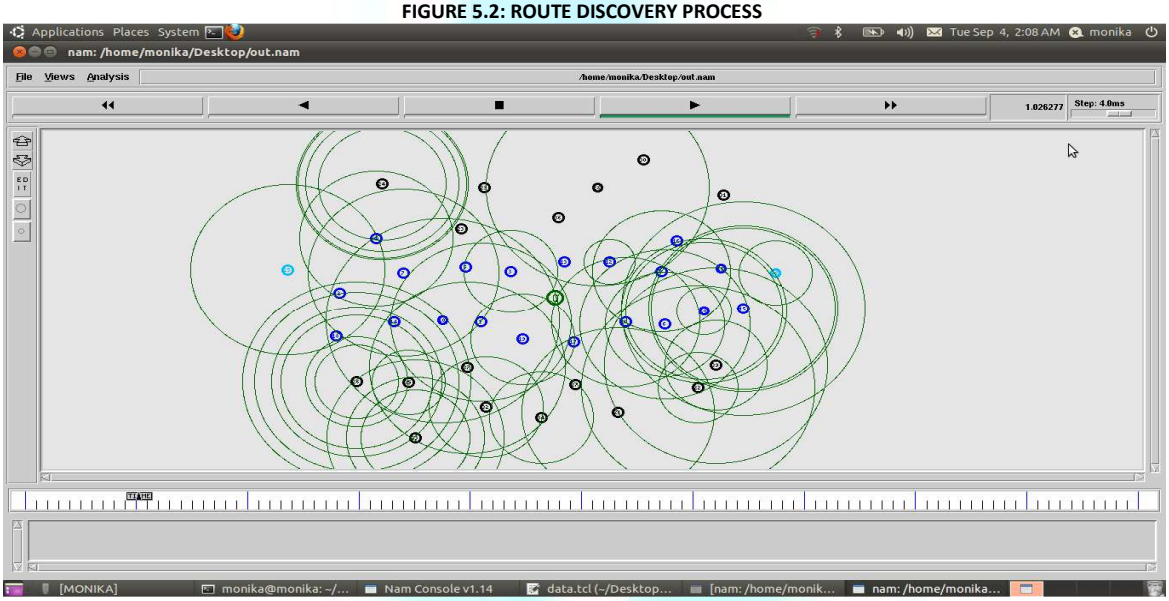


FIGURE 5.3: PACKET LOSS BEFORE ATTACK

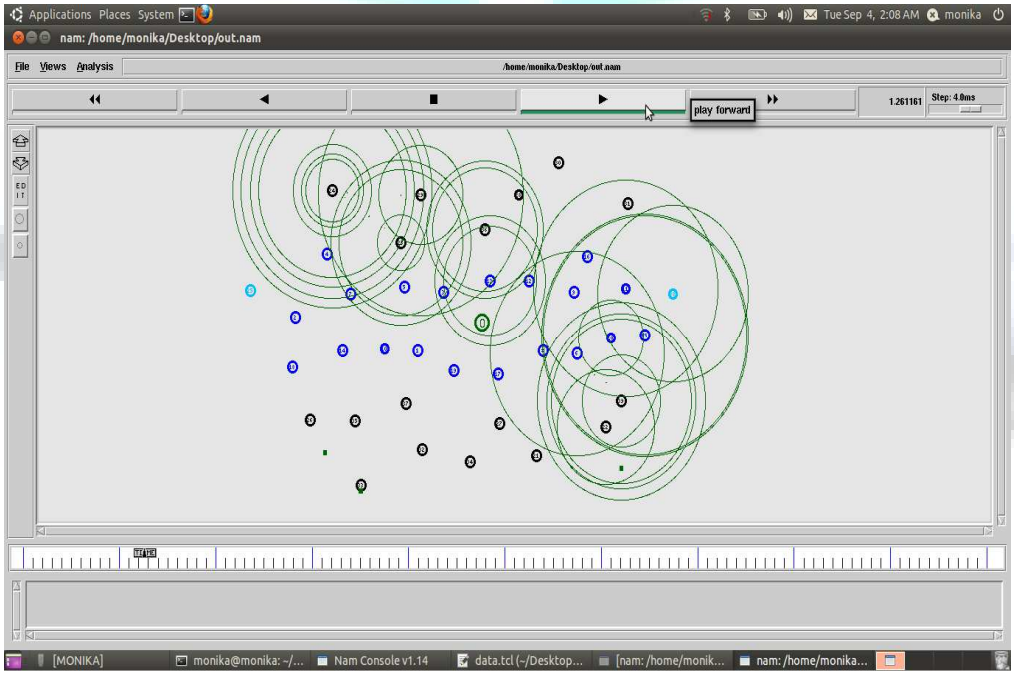


FIGURE 5.4: NODE 36 ACTING AS BLACK HOLE

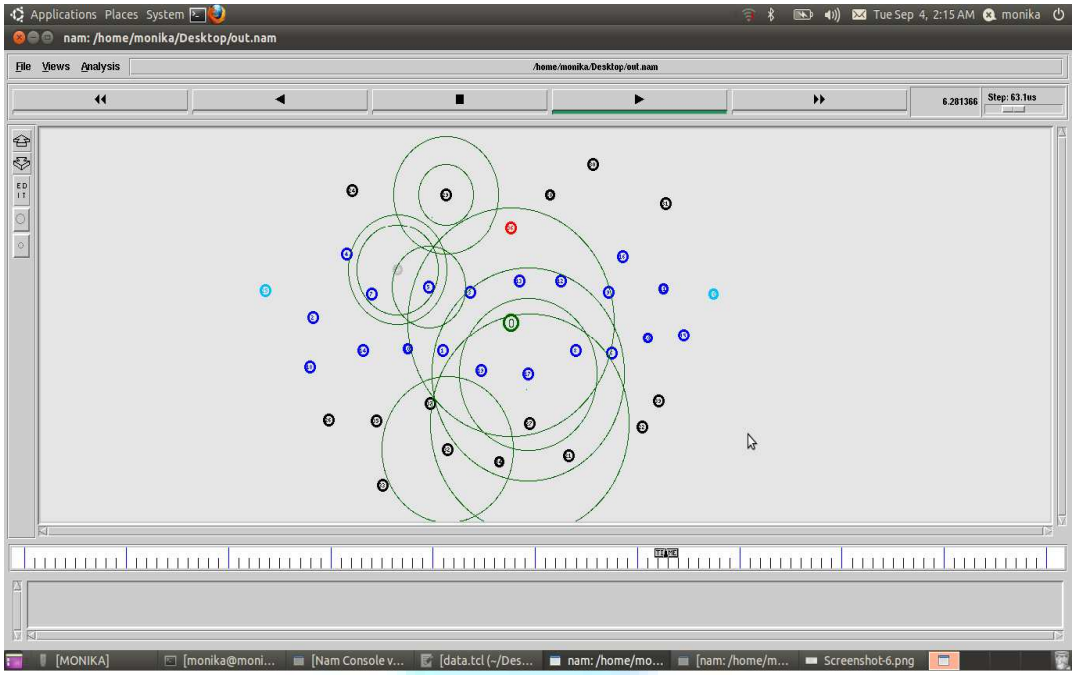
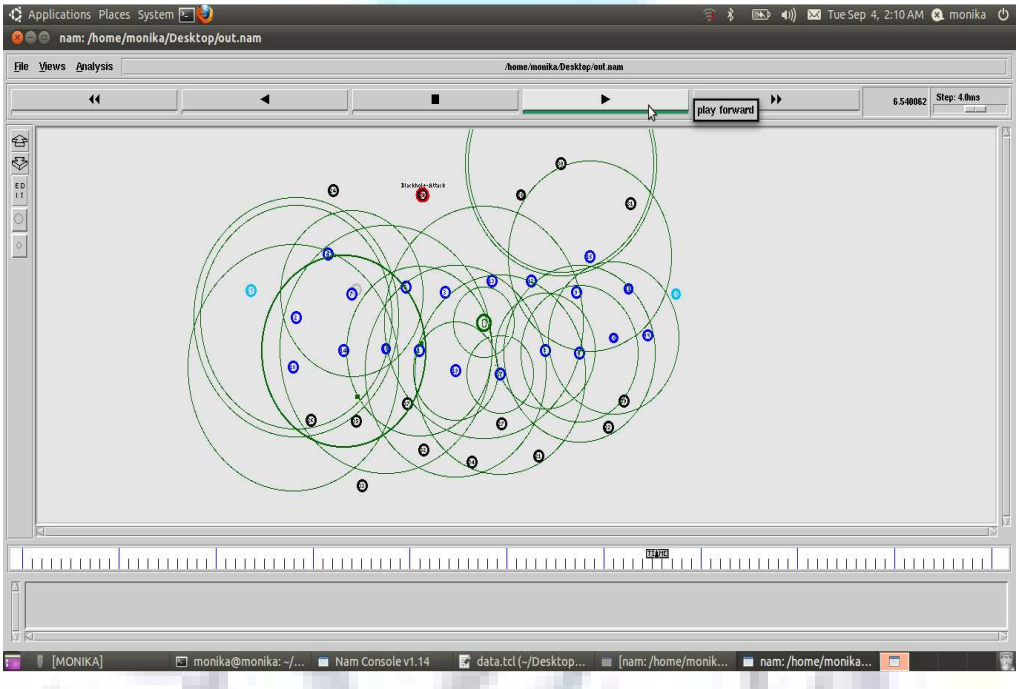


FIGURE 5.5: PACKET DROP AFTER BLACK HOLE ATTACK



We have taken different scenarios of defined parameters for our simulation with or without black hole node. We have taken different positions and movements of nodes for each scenario. Then we had entered the black hole nodes and simple nodes to evaluate the performance. The metrics are used to evaluate the performance are packet loss, throughput and end-to-end delay. We calculate data loss with black hole and without black hole node. Then we compare the results of these two simulations to understand the network and node behaviours. The result of the simulation shows that the packet loss in the network with a black hole increases beyond that dropped without the black hole node.

Our simulation results show that AODV network has normally 2.50 % data loss and if a black hole node is introducing in this network data loss is increased to 89.38%. As 2.50 % data loss already exists in this data traffic, black hole node increases this data loss by 86.88 %.We have also analyzed the throughput of received packets with the presence and absence of black hole node with respect to the simulation time of 450(s) in Figure 5.8. Figure 5.9 illustrates the graphic representation of packet loss percentage with and without black hole node with respect to simulation time.

Figure..8 shows the effect of black hole attack on throughput of received packets of network. The result shows both the cases with black hole and without black hole attack. With our simulation, we analyzed that the throughput of received packets in AODV is very high than the throughput of received packets in black hole AODV. Because the packet loss in black hole AODV is higher than the AODV protocol.

We also studied the performance with varying the number of nodes. Figure.5.7 shows the impact of number of nodes on throughput without black hole attack. The number of nodes is varying from 10 to 40 with the step of 5. Simulation results show that when the number of nodes increases, the throughput increases for AODV protocol.

Figure.5.6 shows the impact of simulation time on throughput and packet delivery ration .It shows that as the simulation time increases the throughput and packet delivery ration also increases as there is low packet loss. This is the case when there in no black hole node in the network.

FIGURE 5.6: THROUGHPUT AND PDR VS SIMULATION TIME FOR AODV

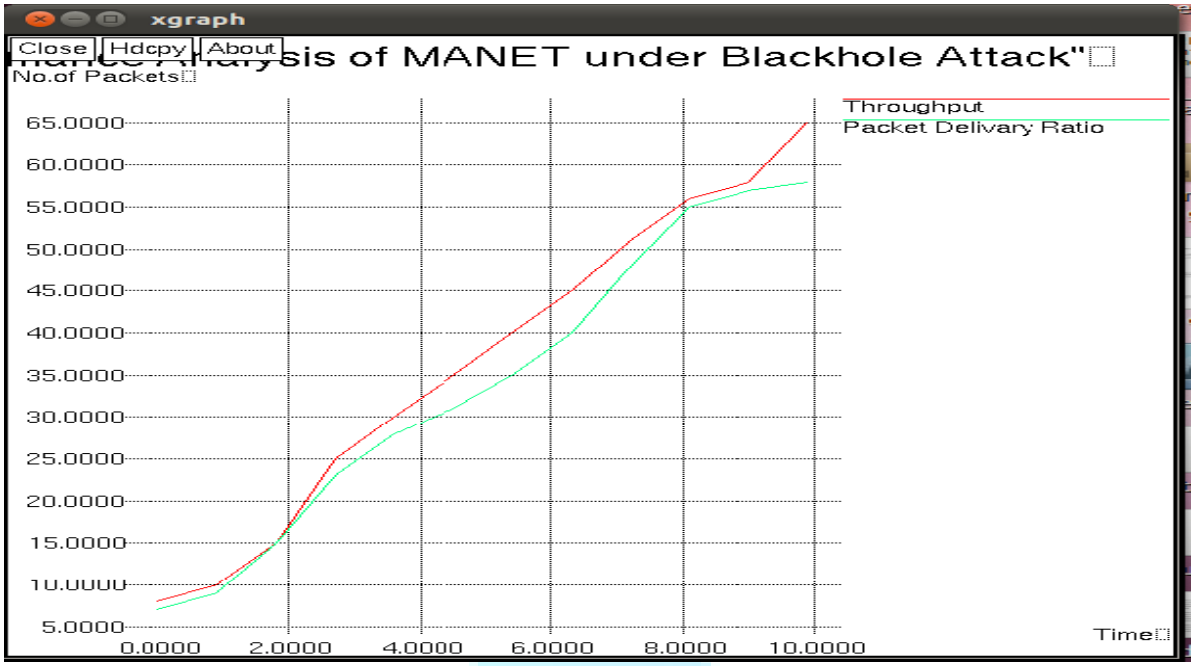


FIGURE 5.7: THROUGHPUT VS NUMBER OF NODES FOR AODV PROTOCOL

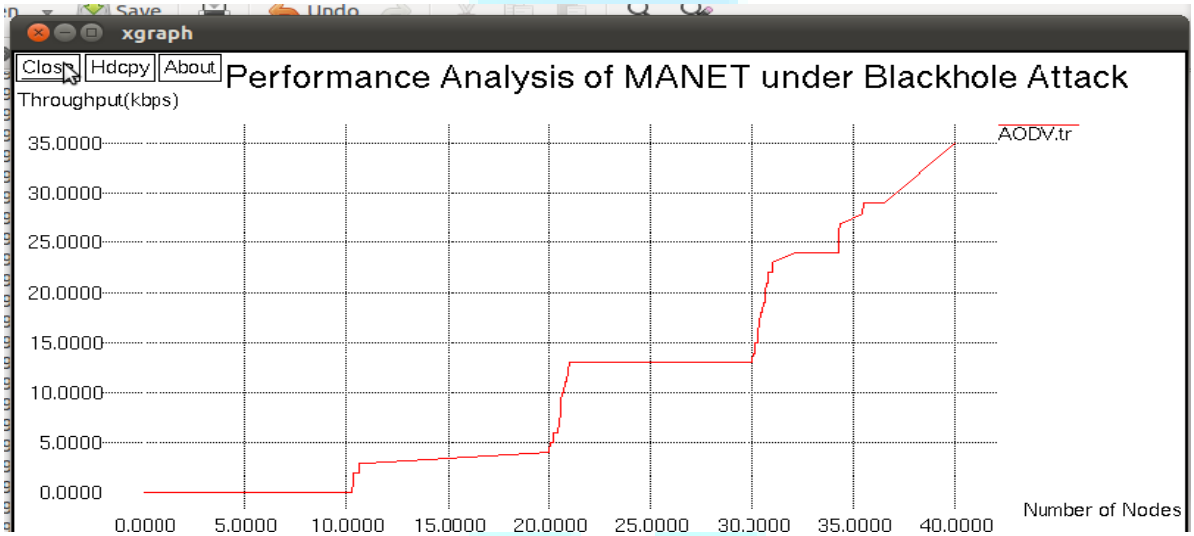


FIGURE 5.8: IMPACT OF BLACK HOLE NODE ON THROUGHPUT OF RECEIVED PACKET

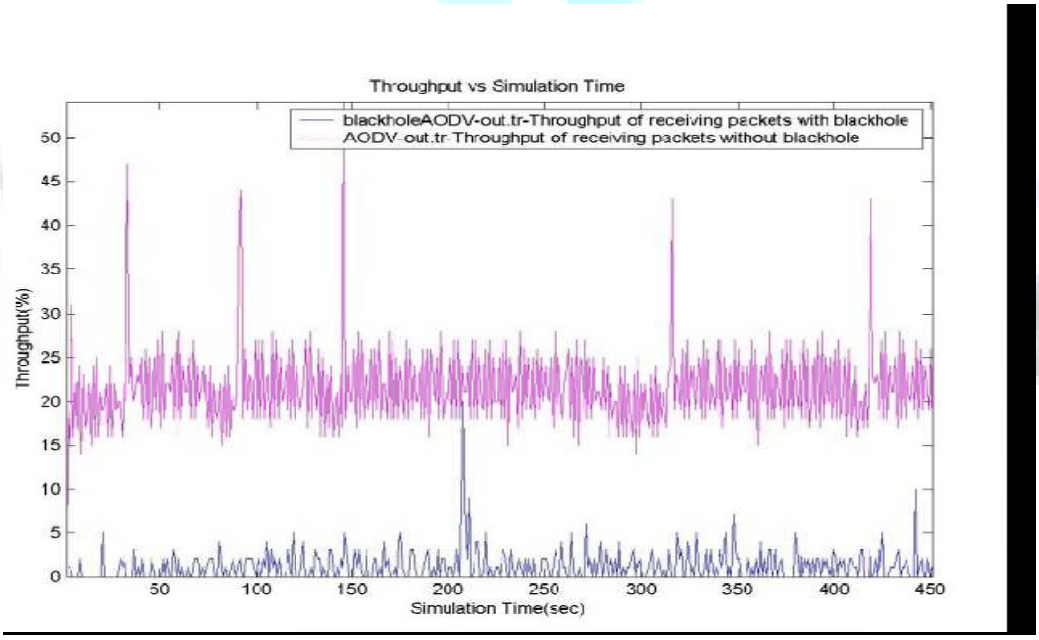
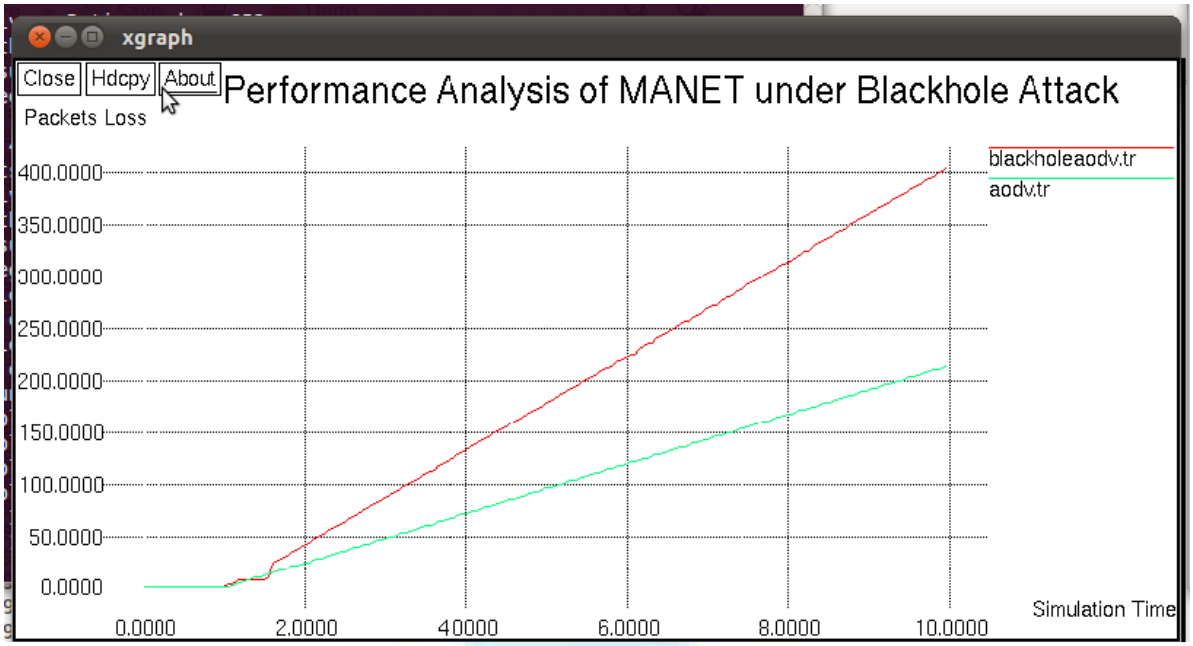


FIGURE 5.9: SHOWS THE PACKET LOSS OF AODV AND BLACK HOLE AODV



6. CONCLUSION

Thus we have analyzed the effect of Black Hole attack on very popular on demand routing protocol AODV, by means of various performance metrics such as PDR, throughput & packet loss, as well obtained simulation results by varying number of nodes in the network & found that there is non linear change in the values of these metrics also we realized that if the number of black hole nodes increased the network performance will be decreased.

7. FUTURE SCOPE

The research on MANET is still in an early stage. Existing proposals are typically based on one specific attack. They could work well in the presence of designated attacks, but there are many unanticipated or combined attacks that remain undiscovered. A lot of research is still on the way to identify new threats and create secure mechanisms to counter those threats. More research can be done on the robust key management system, trust-based protocols, integrated approaches to routing security, and data security at different layers

Mobile Ad Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis we have analyzed the behavior and challenges of security threats in mobile ad hoc networks with solution finding technique with special attention to the black hole attack.

Mobile Ad hoc networks are widely used networks due to their flexible nature i.e. easy to deploy regardless of geographic constraints. These networks are exposed to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still need in this area. We tried to discover and analyzed the impact of black hole attack in MANETs using AODV. There is a need to analyze black hole attack in other MANETs routing protocols such as DSR, TORA and GRP. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with black hole attack. They can be categorized on the basis of how much they affect the performance of the network. The detection of unpredictable behavior of black hole attack as well as the elimination strategy for such behavior has to be carried out for further research.

8. REFERENCES

1. Bala etal Performance Analysis of MANET under Blackhole Attack First International Conference on Networks & Communications 2009,IEEE.
2. C.E.Perkins and E.M.Royer, “Ad-Hoc On Demand Distance Vector Routing,” Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.
3. G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006
4. http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, last visited 12, Apr, 2010.
5. http://www.faqs.org/rfcs/rfc3561.html
6. http://www.isi.edu/nsnam/ns/tutorial/.
7. http://www.isi.edu/nsnam/ns/tutorial/Xgraph utility of ns2
8. K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007.
9. Latha Tamilselvan, V sankaranarayanan, “Prevention of Blackhole Attack in MANET”. In Proceedings of The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), pp. 21-21, Aug. 2007.
10. M. Al-Shurman, S-M. Yoo, and S. Park, “Black Hole Attack in Mobile Ad-Hoc Networks,” ACM Southeast Regional Conf. 2004.
11. S. Kurosawa et al., “Detecting Blackhole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic” .
12. S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.
13. Shurman etal Black Hole Attack in Mobile Ad Hoc Networks ACMSE’04, April 2-3, 2004, USA.
14. Subash Chandra Mandhata and Dr.Surya Narayan Patro A counter measure to Black hole attack on AODV- based Mobile Ad-Hoc Networks International Journal of Computer & Communication Technology (IJCCT), Volume-2, Issue-VI, 2011.
15. The Network Simulator - ns-2; http://www.isi.edu/nsnam/ns/
16. The ns Manual, the VINT project ,october11,2005.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application and Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-

Co-ordinator

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals