Impact of Black Hole and Neighbor Attack on AOMDV Routing Protocol

Priyanka Bansal
Research Scholar (Department of Computer Science & Engineering),
RIMT-IET, Mandi Gobindgarh (147301), Punjab, India.

Prof. Anuj K. Gupta
Professor & Head (Department of Computer Science & Engineering),
RIMT-IET, Mandi Gobindgarh (147301), Punjab, India

Abstract: In Mobile Ad-Hoc Networks (MANETs), security is one of the most important concerns because a MANET's system is much more vulnerable to attacks than a wired or infrastructure-based wireless network. Designing an effective security protocol for MANET is a very challenging task. This is mainly due to the unique characteristics of MANETs, namely shared broadcast radio channel, insecure operating environment, lack of central authority, lack of association among users, limited availability of resources, and physical vulnerability. In this paper, simulation based study of the impact of neighbor attack and black hole attack on AOMDV routing protocol by calculating the performance metrics such as packet delivery ratio, end to end delay and throughput will be presented.

Keywords- MANET, AOMDV, Security, Black Hole Attack, Neighbor Attack.

I. INTRODUCTION

A Mobile Ad hoc Networks (MANETs) is defined as a wireless network of mobile nodes communicating with each other in a multi-hop fashion without the support of any fixed infrastructure such as base stations, wireless gateways or access points. For this reason, MANETs are also called infrastructure-less or non-infrastructure wireless networks. The term ad hoc implies that this network is established for a special, often extemporaneous service customized to specific applications. MANETs enable wireless networking in environments where there is no wired or cellular infrastructure; or, if there is an infrastructure, it is not adequate or cost effective. The absence of a central coordinator and base stations makes operations in MANETs more complex than their counterparts in other types of wireless networks such as cellular networks or wireless local area networks (WiFi networks). Security issues of MANETs in multipath communications [29] are more demanding due to the involvement of multiple paths from source to destination. Although several types of security attacks in MANETs have been studied in the literature, the focus of earlier research is only on unipath applications.

II. REVIEW OF THE STATE OF ART

Previously works reported on MANETs focuses mainly on various security risks and attacks such as DOS attack, Distributed DOS, Impersonation, Wormhole, Jellyfish, and Black Hole attack [4, 5, 8, 13 and 14]. The black hole attack among these other attacks involved in MANET is evaluated based on demand routing protocol like AODV and its effects are clarified by stating how this vulnerable attack disrupt the effective performance of MANET. Very limited attention has been paid to the fact to review the effect of both Black Hole attack and Neighbor attack in MANETs over AOMDV protocol. There is a need to address AOMDV protocol under these attacks, as well as the impacts of these attacks on the AOMDV protocol. So, this paper analyzes Black Hole attack as well as Neighbor attack in MANETs using AOMDV protocol. Despite the fact of popularity of MANET, these type of networks are alot more susceptible to attacks [2, 12]. Wireless links also makes MANET more vulnerable to attacks which makes easier for the attacker to get enter into the network and have malicious access to the communication [2, 11]. Distinct attacks have been evaluated in MANET and their adverse effect on the network. MANETs routing protocols are also being oppressed by the attackers in the form of attack like flooding attack, which is done by the malicious attacker either by using sending RREQ or data flooding [7]. In any network, the operator wants its information to be sent as soon as probable in a protected environment efficiently. Various attackers endorse themselves to have the efficient smallest path and highly available bandwidth available for the communication such as in wormhole attack. The attackers get themselves in robust and important strategic locations in the network and make the best use of their location (i.e. they have shortest path between the nodes) [5, 8]. One of the most issuing matter in MANET is having the insufficient battery, due to this disadvantage the attackers take an leverage of this defect and tries to keep the nodes alive until all energy of the attacked node is extinct and the node go into long- lasting sleep [2]. Distinct other vulnerable attacks in MANET such as jellyfish attack, modification attack and Routing Table Overflow attack have been reviewed and disclosed [24, 6, and 10]. This paper is organized as follow section 3 is about Problem statement and main contribution, section 4 discusses AOMDV, section 5 discusses Black Hole attack, section 6 discusses Neighbor attack, section 7 is about Impact of Attack Simulations and Results and section 8 discusses Conclusion and Future Work.

III. Problem Statement and Main Contribution

Aims and objectives of this study work are summarized as follow:

1. The research targets on analysis of black hole attack and neighbor attack in AOMDV and its consequences.
2. Analyzing the effects of black hole attack and neighbor attack in the light of Network load, throughput and end-to-end delay in AOMDV.
3. Simulating the both attacks using AOMDV routing protocol.
4. Comparing the results AOMDV protocol and impact of attacks on AOMDV protocol.

The fundamental target of any network is to assure the robust communication among the devices in the network of secure environment. So, in ordered to explore, in the case, when there is a malicious attack in the network, the impact as well as effect of the attack and vulnerability of the routing protocols.

IV. AOMDV ROUTING PROTOCOL REVIEW

AOMDV Routing Protocol [23] is one of the most currently used Ad-Hoc routing protocol. This reactive routing protocol based on the DSDV. AOMDV protocol is created for network systems with tens to thousands of mobile hops. The main concept in AOMDV is to compute or produce multiple paths during route discovery process. It is created mainly for highly dynamic ad-hoc type of networks where the link failures as well as route breaks take place usually. When single path protocols like reactive routing protocol such as AODV is when used in such type of networks, a new route discovery is required in response to each route break. Every route discovery is correlated with high overhead and latency. This inability as well as inefficiency can be evaded or avoided by having the numerous (multiple) redundant paths availability. The AOMDV protocol has two phases:

1. A route updating rule to create and manage multiple loopfree paths at every hop.
2. A distributed protocol to find out the node-disjoint paths that is route discovery.

In AOMDV a new route discovery is required only when all the paths leads to the destination break. Main characteristics of the AOMDV protocol is the usage of routing information that is earlier available in the basic AODV protocol as much as possible. Therefore little additional overhead is enforced for the computation of multiple paths.

A. Route Discovery-

The route discovery process has broadly two aspects: route request and route reply aspect. The route discovery process computes the multiple loop free paths. The route discovery process will be started only when a route is desired by a source hop and there is no data about the route in its respective routing table. Firstly, source hop set up an RREQ and then deluge the packet to the networks. The RREQ's are propagated to neighbours within the source's transmission spectrum. They also renounce the packets to their respective neighbours. The operation is replicated till the destination accepts the RREQ. When an intermediate node accepts the RREQ, it performs the following procedure:

1. When an intermediary hop gets the information of RREQ, either it transmit the route reply if the hop is the destination, or it renounce the RREQ to it neighbours.

2. The hop scans the required information from the RREQ.

In order to transfer route reply packets to the source hop, the hop makes a reverse path to the source hop. The hop will embed the path to its numerous multiple path lists. Otherwise, the hop will avoid the path and abandon the RREQ.

Link failures in ad-hoc networks are induced by mobility, congestion, packet collisions, node or hop failures etc. The link layer in the AOMDV protocol evaluated from IEEE 802.11 is utilized to detect or reveal link failures. If a hop delivers packets along the broken link, it will be accepted or received by a link layer feedback. When a hop reveals a link break, it broadcasts as well as announces route error (RERR) packets to its neighbours. The neighbours then rebroadcast and renounce the packets until the entire source hops get as well as receive the packets. If a source hop accepts the RRER, it will discard each entry in its respective routing table that takes the usage of the broken link. As compare from single-path routing protocols, the routes having error packets should consist of the crucial information not only about the broken primary paths but even the broken backup routes. When the source originated hop gets the RERR's, it discards all smashed routing entries and utilizes the shortest backup paths as initial paths. The source hop originates a route discovery process where all the backup paths are broken.

B. Benefits and Limitations-

AOMDV is on demand reactive routing protocol which determines the route as and when needed by sending packets to its neighbors. AOMDV choose the most optimum path from available paths between source node and destination node. The optimization criteria can be shortest and least congested path.

V. BLACK HOLE ATTACK

It is a type of attack in computer networking that forms the DOS attack in which router is supposed to broadcast packets instead of abandon them [16]. This generally occurs from a router that becomes settled from a number of different causes. Because packets are routinely released from lossy network, so packet drop attack is very challenging to uncover and prevent.

The fake router can also accomplish this attack, for exemplar: by drop packets for particular network destination, at any time of day, a packet with every n packet or every second, or randomly selected portion of packets. So this is reasonably called gray hole attack. Also, if the vicious routers attempt to drop all packets that come in, then attack can actually be observed fairly as well as fast through common networking tools such as trace route. Further, even when other routers notice that settled router is dropping all traffic, they will begin to suppress that router from their forwarding tables and as a result no traffic will flow to attack. However, if malicious router begins to drop packets on definite time period or over every n packet, it is generally callous to detect as some traffic still flows across the network. Packet drop attack can frequently deployed to attack wireless adhoc networks. Wireless networks have much different architecture than that of typical wired network, a host can newcast that it has the shortest path towards destination. By doing it, all traffic will be directed to appropriate host that has been ruined, and the host will be able to abolish packets. Also over Manet, hosts are specifically susceptible to collectively attacks where multiple hosts will become compromise and betray the other hosts on the network.

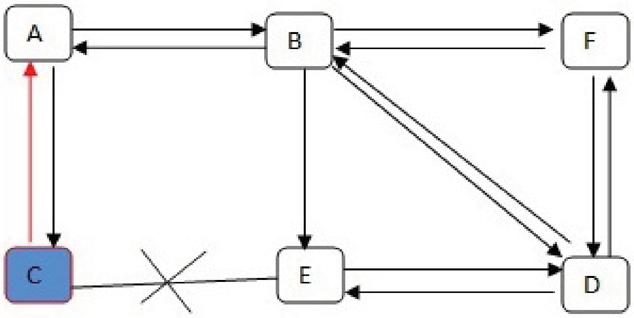


Figure1. Black hole attack in AOMDV

VI. NEIGHBOR ATTACK

The fundamental objective of the neighbor attack is to disrupt the multipath paths by making two hops that are in fact out of each other's transmission spectrum consider that they can transmit the data directly with each other [15]. If these two hops are part of network routing mesh, the join reply packages that they swap will be extinct because there is no actual existing connection and transmission between them. A neighbor attacker disrupts the routing protocol and doesn’t requirement to engage itself later in the package dropping mechanism, since the package will be vanished eventually due to the imitating links. Upon receiving a packet, an intermediate node records its IP in the packet before forwarding the packet to the next node. However, if attacker only delivers the packet even without recording its IP in the packet, it makes two hops that are not within the transmission spectrum of each other belief that they are neighbors, resulting in a disrupted route. Run experiments with neighbor attacks has implemented, and used the simulation setting as shown in Figure 2 shows an example of neighbor attack where, Source node S sends Join Query to the Destination node D through its neighbor nodes J and M, when the Attacker node A receives a Join Query it forward to the node K without updating the previous hop field which makes fake link i.e., the nodes J and K assume that they are having link between them. But there is no actual connection between them. Hence the join reply packet form the node D will be extinct because there is no originality in connection between them.

Using simulation, study how the number of attackers and their positions affect the performance of a multipath session in terms of packet delivery ratio, throughput, control overhead, and end-to-end delay. Our simulation results show that a large multipath group with a high number of senders and/or a high number of receivers can sustain good performance under these types of attacks due to several alternative paths in the routing mesh. The most damaging attack positions are those close to the senders and around the mesh center.

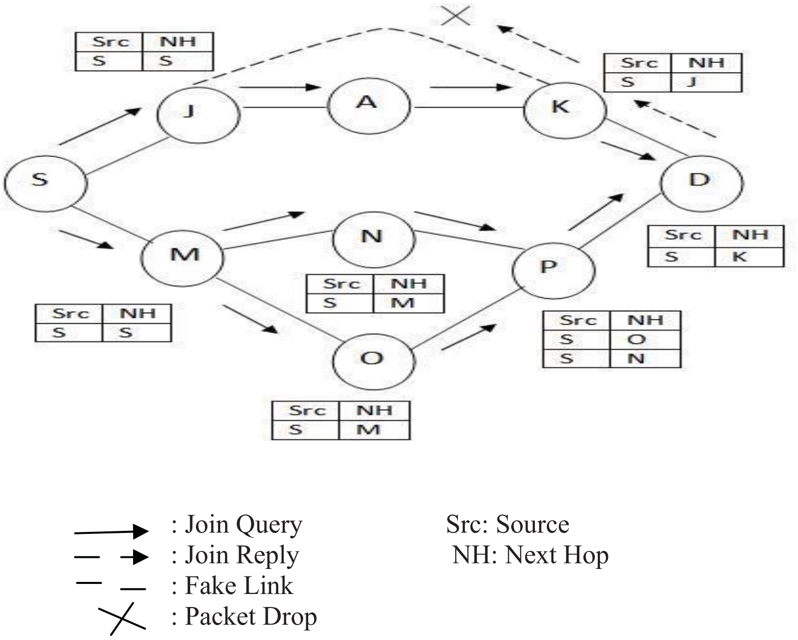


Figure 2. Neighbor attack

VII. IMPACT of ATTACKS SIMULATION and RESULTS

Black hole attack and Neighbor attack has been implemented in an ns2 simulator [15]. Impact of these attacks on AOMDV protocol will be compared with AOMDV protocol without attacks. The problem formulation is reviewed emphatically by compiling data, various experiments and simulation which gives some results then these results are evaluated and opinions and judgments are made on this criteria. To analyze the effective performance as well as results of a protocol for adhoc network, it is significant to evaluate it under practical conditions, especially including the movement of mobile-hops. The simulation demands to initiate traffic and mobility model for performance evaluation process. Following table shows the traffic scenario.

A. TRAFFIC SCENARIO-

Table 1. Shows Traffic Scenario

ROUTING PROTOCOL	AOMDV
ATTACKS	BLACK HOLE ATTACK, NEIGHBOR ATTACK
AREA	1000mX1000m
TRAFFIC TYPE	CBR, TCP
VELOCITY	8.32m/sec
PACKET SIZE	512
NUMBER OF NODES	50
SIMULATION TIME	50 sec

For the evaluation following metrics will be used:

1. **Packet Delivery Ratio (PDF):** It is the ratio of the packets received by destination to those generated by the sources. CBR traffic type is used by source. It specifies the packet loss rate, which restricts as well as limit the maximum throughput of the network. The routing protocol which have better PDR, the more complete and correct. This reflects the usefulness of the protocol. And provide good performance.

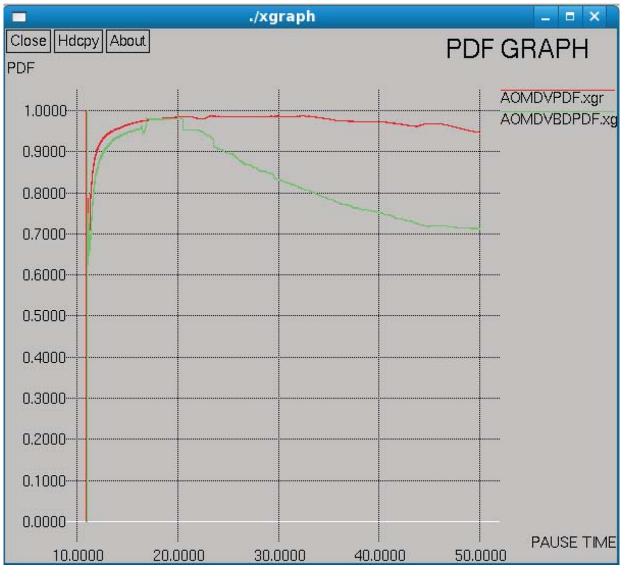


Figure 3. PDF Graph

2. **End to End Delay:** Average ee-delay is the average time taken by the packet to reach to destination in seconds.

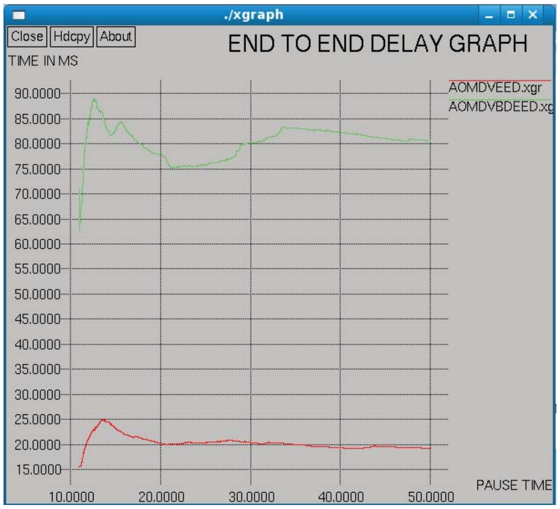


Figure 4. End to End Delay Graph

3. **Throughput:** No. of packet passing through the network in a unit of time. It is measure in kbps.

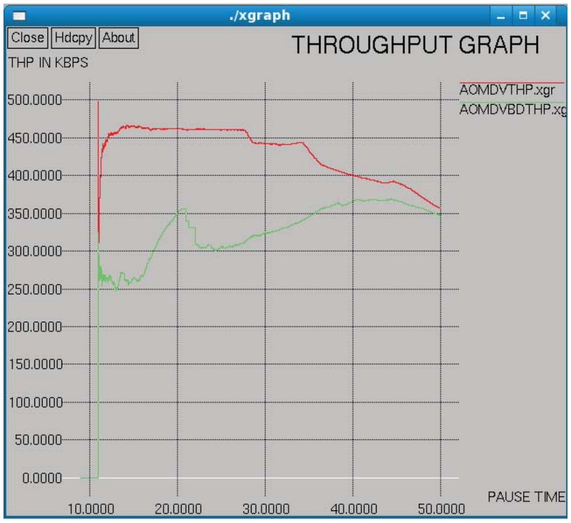


Figure 5. Throughput Graph

B. Experimental Process-

The simulation scenario and parameters used for performing the detailed analysis and study of Black hole attacks and Neighbor attacks on MANET protocols is described below. This facet represents that how the effective performance parameters have been analyzed to simulate the protocols.

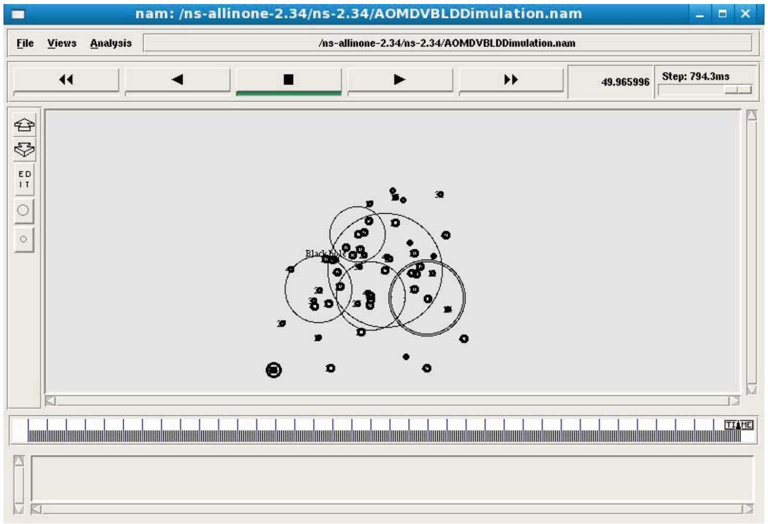
Following steps have been used for simulation.

1. *Inputs to Simulator:-*
    - Scenario File – Movement of nodes.
    - Traffic pattern file.
    - Simulation TCL file
2. *Outputs File from Simulator:*
    - Trace file
    - Network Animator file

3. *Output from Trace Analyzer:*
    - xgr file

C. NAM (Network Animator)–

NAM stands for Network Animator. It has data for network topology and shows graphical representation. It begins with the proceeding command 'nam <nam-file>' where '<nam-file>' is the name of nam trace file i.e. .tr file. At linux terminal, the command to run NAM is ./nam.



nam: /ns-allinone-2.34/ns-2.34/AOMDVBLDDimulation.nam

/ns-allinone-2.34/ns-2.34/AOMDVBLDDimulation.nam

49.965996

Step: 794.3ms

Figure 6. NAM

After performing simulation as per network scenario, trace files are produced. Trace file have following information:

1. Send/Receive Packet
2. Time
3. Traffic Pattern
4. Size of Packet
5. Source Node
6. Destination Node etc.

D. Analysis done using Trace Analyzer-

Awk scripts i.e. awk files trace analyzer is used to evaluate trace outputs from simulation. When files are evaluated using this trace analyzer then an output .xgr file is produced which results in the creation of graphs i.e. xgraphs.

E. SIMULATIONS RESULT TABLE-

Table 2- Shows Result Table

ROUTING PROTOCOL	AVERAGE END TO END DELAY in ms	AVERAGE PACKET DELIVERY FRACTION RATIO (%)	AVERAGE THROUGHPUT in kbps
AOMDV	19.21 ms	0.95 %	357.22 kbps
AOMDV WITH NEIGHBOR AND BLACK HOLE ATTACK	80.6 ms	0.71 %	347.85 kbps

F. COMPARISON-

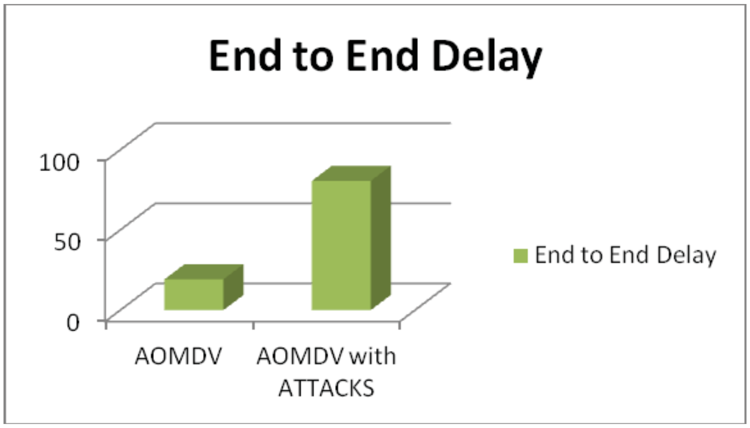


Figure 7. End to End Delay Comparison

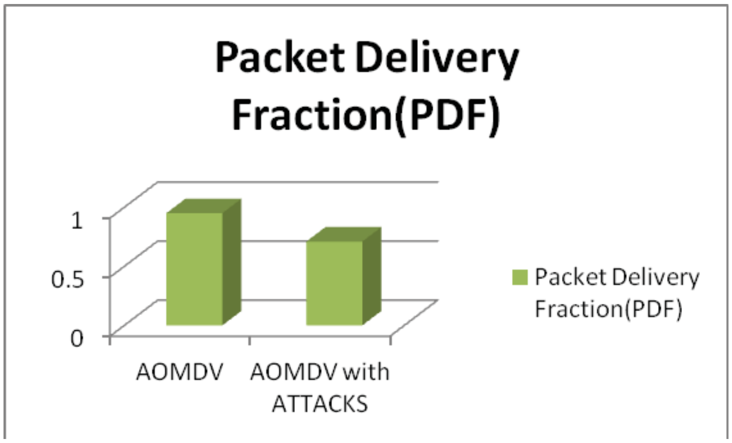


Figure 8. Packet Delivery Fraction Comparison

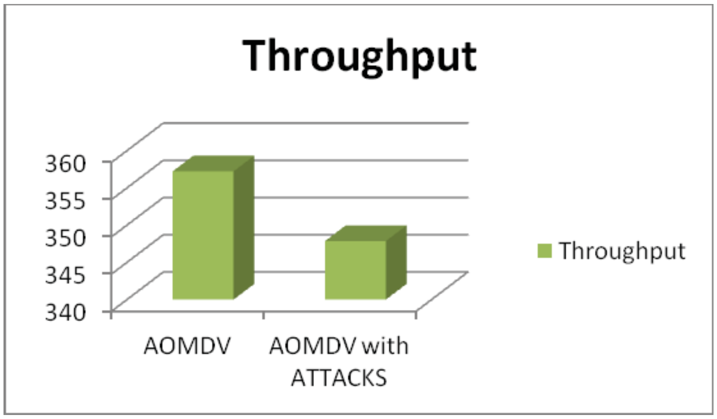


Figure 9.Throughput Comparison

VIII. CONCLUSION and FUTURE WORK

In this paper, the Black hole attack and Neighbor Attack have been analyzed in order to calculate average of distinct efficient performance parameters such as end-to-end delay, throughput and packet delivery ratio. This research has done to evaluate the effect of Black hole attacks and Neighbor attack on the performance of AOMDV protocol. So the impact of attacks is very much vulnerable to AOMDV protocol. So there must be some techniques that avoid these vulnerable attacks and make the protocols secure by reducing the overheads that can occur by implementing security techniques like P.G.P. with load balancing.

IX. ACKNOWLEDGEMENT

This research paper is made possible through the help and support from everyone, including: parents, teachers, family, friends, and in essence, all sentient beings. First and foremost, I would like to thank Mr. Anuj K. Gupta for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper. Finally, I sincerely thank to my parents, family, and friends, who provide the advice and financial support. The product of this research paper would not be possible without all of them.

REFERENCES

[1] Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: Secure On-demand Protocol for AdHoc Networks. In Proceedings of the Eighth ACM Annually International Conference on MANET, pages 12–23, September 2002.

[2] P.V.Jani, “Security within AdHoc Networking,” Position Paper, PAMPAS Workshop, Sept. 2002.

[3] M.Parsons, P.Ebinger, “Performance Evaluation about the Impact of Attacks on MANETs,” [Online].

[4] D.B.Roy, R.Chaki and N.Chaki, “A New Cluster-Based Wormhole IDS Algorithm for MANETS,” The International Journal for Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.

[5] H. Nguyen, U. Nguyen, “Reviewing of Different Types of Attacks on Multipath in MANETS,” International Conference on System and Networks and International Conference Based on Mobile Communications and Learning Tech. (ICN /MCL 2006), pp.149- 149, April, 2006.

[6] Wei, Xiang, B.yuebin and Xiaopeng, “New Solution about Resisting Gray Hole Attack in MANETs,” 2nd International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.

[7] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, “A Reputation-Based Mechanism for Isolating Selfish hops in AdHoc Networks,” 2nd International Conference on Mobile & Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[8] V.Mahajan, M.Natue and A.Sethi, “Analysis of Wormhole Intrusion attacks in MANETs,” IEEE Military Communications Conference, pp. 1-7, Nov, 2008.

[9] F.Stanjano, R.Anderson, “The Resurrecting Duckling: Security Issues for Ubiquitous Computing,” Vol. 35, pp. 22- 26, Apr, 2002.

[10] H.Deng, W.Li and D.P.Agrawal, “Routing Security in Wireless Networks,” University of Cincinnati, IEEE Communication Magazine, Oct, 2002.

[11] K. Biswas and Md. Liaqat Ali, “Security against threats in MANET”, Master of Thesis, Blekinge of Technology” Sweden, 22nd March 2007.

[12] Lu, Li, K. Lam, L. Jia, “SAODV: A MANET Protocol that can with Black Hole Attack.,”

[13] Kai Wang, Jia Chen, Huachun Zhou and Yajuan Qin,”Content-Centric Networking: Efect of Content Cachingon Mitigating DoS Attack”, International Journal of Computer Science Issue, pp.43-52, vol.9, (6-3),November2012

[14] L.Zonglin, H.Guangming, Y.Xingmiao, “ Spatial Correlation Detection of DDoS attack” International Conference on Communication, Circuits and System (ICCCAS 2009), pp. 304-308, July, 2009.

[15] S. Parthiban, A. Amuthan, N.Shanmugam and K.Suresh Joseph:”NEIGHBOR ATTACK AND DETECTION MECHANISM IN MANETs”. In proceedings of the Advanced Computing: An International Journal (ACIJ), Vol.3, No.2, March 2012.

[16] B.Revathi et.all, “A Survey of Cooperative Black and Gray hole Attack in MANET,” International Journal of C.S. And Management Research Vol 1 Issue 2 September 2012 ISSN 2278-733X.

[17] Deepak KR T.V.P.Sundararajan,”An Immune Inspired Approach for Detecting Packet Drop attacks service in MANET” International Journal of Computer Applications (0975 – 8887) Volume 58– No.8, November 2012

[18] Imad Aad Jean-Pierre Hubaux Edward W. Knightly,”Impact of Denial of Service Attacks on AdHoc Networks”, http://citeseerx.ist.psu.edu/viewdoc/doi=10.1.1.74.3839&rep=rep1&type=pdf

[19] Mieso K. Denko,”Detection and Prevention of Denial of Service (DOS) Attacks in MANETs using Reputation-Based Incentive Scheme.” http://rise.cse.iitm.ac.in/wiki/images/3/35/Rep5.pdf

[20] Irshad Ullah ET. all, “Effects of Black Hole Attack on MANET Using Reactive and Proactive Protocols” IJCSI International Journal of C.S. Issues, Vol. 10, Issue 3, No 1, May 2012 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784

[21] D. Johnson,”T he Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4.” February, 2007, [online]. Available : http://tools.ietf.org/html/rfc4728.html

[22] Abhishek Gupta,”Detection and Prevention of Selfish hops in MANET using Innovative Brain Mapping Function: Theoretical Model.” International Journal of Computer Applications (0975 – 8887) Volume 57– No.12, November 2012

[23] Marina, M. K. and Das, S. R., “On-demand Multipath Distance Vector Routing for Ad Hoc Networks,” Proc. of 9th IEEE Int. Conf. On Network Protocols, pp.14-23 (2001)

[24] H...Nguyen, U .Nguyen, “Study of Different Types of Attacks on Multipath in MANET,” International Conference on Networking, Mobile Communications & Learning Technologies, Apr, 2006.

[25] Tamilselvan, & Sankaranarayanan, Prevention of Black hole attack in MANET. 2nd International Conference on Wireless Broadband & Ultra Wideband Communications, 21-21, 2007.

[26] Dokurer; Ert, M.; and Acar, E., Performance analysis of adhoc networking under Black hole attacks. Southeast Con, 2007, Proceedings IEEE, 148 – 153.

[27] C. Perkins; E Belding-Royer; and S. Das (2003) AODV routing. RFC 3561. The Internet Engineering Task Force, Network Working Group.

[28] Sheenu Sharma, Dr. Roopam Gupta-Simulation Study of Black hole Attack in the MANET, November 2009.

[29] Anuj K. Gupta, Harsh Sadawarti -Secure Routing Techniques for MANETs, International Journal of Computer Theory and Engineering (IJCTE), ISSN: 1793-8201, Article No. 74, Vol.1 No. 4, pp. – 456-460, October 2009.

[30] Nital Mistry, Devesh Jinwala, Mukesh Zaveri- Improving AODV Protocol against Black hole Attacks, Proceedings of the international multi conference of engineer and computer science vol. 2, 2010.

[31] Dr. Harsh Sadawarti and Anuj K. Gupta, Member, IAENG- Secure Routing Techniques for MANETs, International Journal On Computer-Theory and Engineering, Vol. 1, No. 4, 1793-820, October2009

[32] Anuj K. Gupta- Secure Routing Techniques for Mobile Ad Hoc Networks, 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6–7March 2009

[33] Anuj K. Gupta, Harsh Sadawarti and Anil K. Verma - Effect of Mobility Parameters on the Performance of AODV Routing Protocol, International Journal of Network and Mobile Technologies ISSN 2229-9114 Electronic Version VOL 3 / ISSUE 1 / JANUARY 2012.

[34] Dr. Harsh Sadawarti, Anuj K. Gupta-Security aspects in ad hoc network routing, Proceedings of International Symposium on Computing Engineering & Technology (ISCET 2010) Mandi Gobindgarh India, 19–20March 2010.