IJCSC 0973-7391 Volume 6 • Number 2 April - Sep 2015 pp. 36-41

International Journal of Computer Science & Communication

Volume 6, Issue 2, April-September 2015

ISSN: 0973-7391 Impact Factor: 2.5 Available at www.csjournals.com

SCAODV: A Protocol to Prevent Black Hole Attacks in Mobile Ad Hoc Networks

\Shailja Sharma[2] ,Umesh Kumar Singh[1], Kailash Chandra Phuleriya[1] & D.N. Goswami[2]
[1]Institute of Computer Science, Vikram University, Ujjain (M.P.)
[2]School of Studies in Computer Science, Jiwaji University, Gwalior (M.P.)

Abstract: A Mobile Ad hoc Network (MANET) is a self-organized wireless short-lived network consisting of mobile nodes. Therefore, security in MANET is the most important concern for the basic functionality of network. MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. In this paper, we have examined certain collaborative attacks prevention routing protocols. Then, we have compared some routing protocols using some identified parameters and finally on the basis of our previous study we have proposed Secure Communication AODV (SCAODV). Further, we have addressed major issues related to this.

Keywords: MANETs, Attacks, Protocol, Routing Protocols, simulation etc**.**

I. Introduction

Mobile Ad Hoc Networks (MANETs) has become one of the most important areas of research in the recent years because of the challenges it pose to the related standards. MANET is the new up-and-coming technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network. An ad hoc network is self-organizing and adaptive. Device in MANET should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service [1-4]. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network.

These factors have made MANETs to receive great attentions and also because of their capabilities of self-configuration and self-maintenance. Another unique feature of MANETs that poses security threats is its unclear defense line; i.e. no built-in security. MANETs does not have dedicated routers and switches, its nodes usually operate by forwarding the packets to one another thereby having no security in the communication; granting access to both legitimate users and attackers. For example, node S can communicate with node D by using the shortest path S-A-B-D as shown in Figure 1 (the dashed lines show the direct links between the nodes). If node A moves out of node S' range, he has to find an alternative route to node D (S-C-E-B-D).

Therefore, security in MANETs is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats [5].

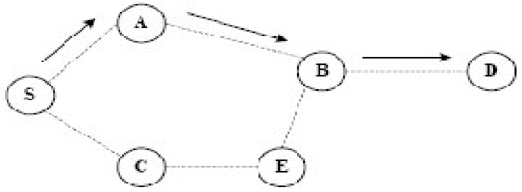


Figure.1: Communication between Nodes on MANETs

A MANETs 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.

The rest of the paper is organized as follows. In Section II, we have described related works. In section III, we described the classification of security attacks. Next, in Section IV, we have showed the best protocol to prevent Black Hole Attack. In section V we describe our proposed work. In section VI we mentioned Results and Discussion. Finally, section V has concluded our work.

II. Related Works

In the last few years, security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However, mobile Ad-Hoc networking is still in need of further discussions and development in terms of security. With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. The comparison of wired network Mobile Ad-Hoc network is different. The routing protocols designed majorly for internet is different from the mobile Ad-Hoc networks (MANETs).

Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks. Major vulnerabilities which have been so far researched are mostly including selfishness, dynamic nature, and severe resource restriction and also open network medium. In MANETs, there are attacks which can be categorized in Passive, Active, Internal, External and network-layer attacks, Routing attacks and Packet forwarding attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANETs are free to move, join or leave the network in other words the mobile nodes are autonomous. Many studies on MANETs focus on the protocols used their security issues such as data encryption, authentication, trust, and cooperation among nodes, attacks on the protocols and proposed solutions or preventions [6-10]. In the face of the different specific attacks on MANET such as Denial-of-Service (DoS), impersonation, Node hijacking and so on that have been exposed [11], the attacks involving multiple nodes seem to have received little attention.

In a black hole attack, several malicious nodes falsely claim a new route to the destination in order to absorb all packets coming from the source. To combat this kind of routing protocol attack, Deng et al. proposed a solution that revolved around waiting and checking the replies from all other neighboring nodes and then deciding on the safe route. Using a fidelity table is another solution, in which every node will be assigned a fidelity level and the node with "0" level will be considered as malicious and be eliminated from the MANETs [12]. Distributed Denial of Service (DDoS) attack is another kind of attack on multiple nodes; it is because of the nature characteristic of this attack. DDoS attack involves breaking into hundreds or thousands of machines and from those machines, attacker launches several attacks aim at target machine in order to consume bandwidth and create bottleneck in the network [13]. In addition, there are different categories of attacks against MANETs. These categories in pair are Passive and Active attacks, Internal and External attacks and the two categories of network-layer attacks: Forwarding attacks [14, 6, 9].From our perspectives, collaborative attacks are non-single attacks; they are attacks launched in multiple malicious nodes acting as a group. Typical examples of these kinds of attacks are Black hole attack, Sybil attack and Wormhole attack on nodes in a MANETs.

Previous studies show that there are different categories of attacks on MANETs, such as Passive and Active attacks, Internal and External attacks and the Routing and Packet Forwarding attacks. Some of these attacks are termed as single attacks while some are referred to as attacks on multiple nodes and are malicious. MANETs is open to vulnerabilities as a result of its basic characteristics like: no point of network management, topology changes vigorously, resource restriction, no certificate authority or centralized authority, to mention a few.

III. Classification of Attacks

Due to the fact that MANET is a group of nodes that form a temporary network without centralized administration, the nodes have to communicate with each other based on unconditional trust. This characteristic leads to the consequence that MANET is more susceptible to be attacked by inside the network while comparing to other type of networks.

A complete picture of attack types on layers is helpful for the effectively mitigations of these attacks. In figure-2, attacks on layers are broadly classified for this purpose

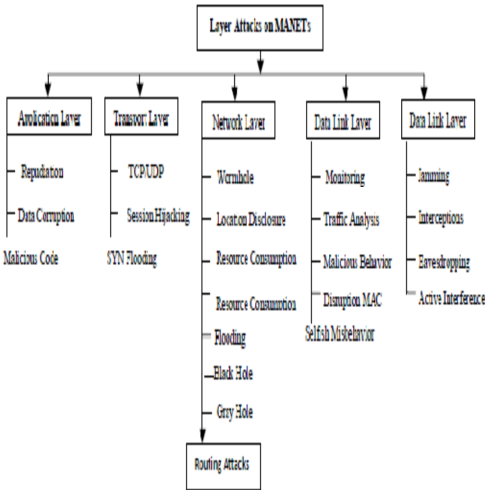


Figure 2: Attacks in various layers of MANETs.

Attacks can also be categorized on the basis of its source, behavior and nodes. Figure-3.1 shows such categorization:

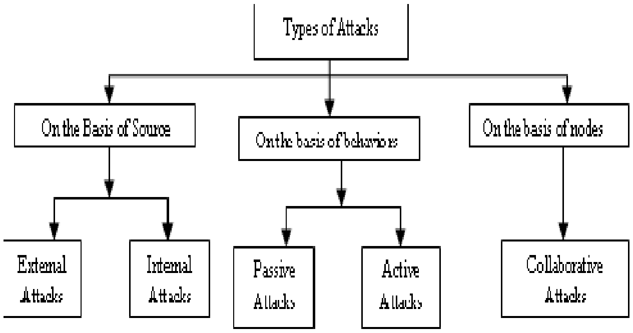
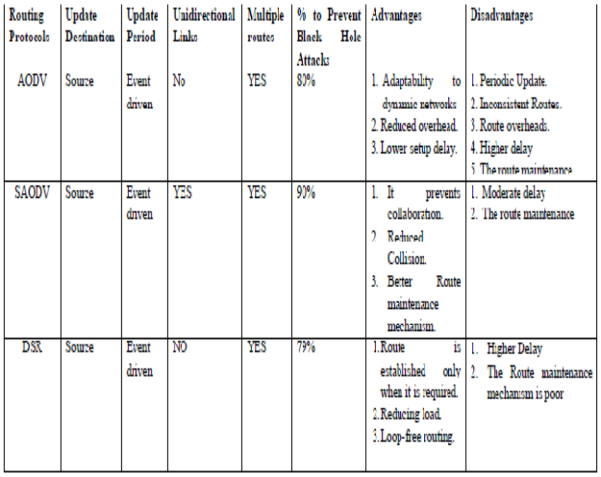


Figure 3: Categorization of Attacks in MANETs

In this study we found that most of the work on MANET security focused on single layer attacks i.e. active and passive attacks. In the meanwhile some attacks involving multiple nodes have received little attention since they are surprising and combined attack i.e. collaborative attacks. There have been no proper definition and categorization of these kinds of collaborative attacks in MANETs. Thus, protection of communication system against these types of attacks is a challenging task. Therefore, deep study on collaborative attacks and development of new protocols/algorithms/model to manage these attacks is the need of hour. Development of a multi-fence security solution that is embedded into possibly every component in the network, resulting in depth protection that offer multiple line of defense against many known and unknown security threats is also given importance.

IV. Protocols to Prevent Black Hole Attack

In [15], singh et al discuss some important routing protocols are used to prevent black hole attacks in MANET. In these protocols he compares using some parameters and the results are shown in following table 1.



Routing Protocols	Update Destination	Update Period	Uidirectional Links	Multiple routes	% to Prevent Black Hole Attacks	Advantages	Disadvantages
AODV	Source	Event driven	No	YES	80%	1. Adaptability to dynamic networks 2. Reduced overhead. 3. Lower setup delay.	1. Periodic Update. 2. Inconsistent Routes. 3. Route overheads. 4. Higher delay 5. The route maintenance
SAODV	Source	Event driven	YES	YES	90%	1. It prevents collaboration. 2. Reduced Collision. 3. Better Route maintenance mechanism.	1. Moderate delay 2. The route maintenance
DSR	Source	Event driven	NO	YES	79%	1.Route is established only when it is required. 2.Reducing load. 3.Loop-free routing.	1. Higher Delay 2. The Route maintenance mechanism is poor

In this comparison, he described the black hole attack that can be increased against a MANET, and compare the some black hole attack preventing routing protocols using the performance results of network simulator. Our study we found than the SAODV protocol provides a batter security as compare to AODV and DSR but not some cases this scheme is liable. So we claim that no such schemes are available to prevent black hole attack without affecting the performances of network. In future we will develop a new scheme for MANET that provides better performance as compare to other schemes.

V. Proposed Work

In our above study we find out the effect of black hole attack on MANET. We simulated the MANET scenarios with and without a black hole node present in the network. On the basis of our study we claim that no such schemes are available to strongly prevent black hole attack. So we introduced a new approach, which we called "Secure Communication AODV (SCAODV). This new approach, secure communication AODV (SCAODV) is inherited from the existing modified AODV and AODV routing protocol.

SCAODV, Root nodes are created first. Root nodes are used for detection of malicious nodes. From source node RREQ is generated. At that time one timer is used for measuring current time. We can assume any expired time. If RREP received before expired time then one fake packet will send to the destination, this packet is not original data packet. After that if acknowledgement (ACK) receives then original packet will send by source node. If ACK not receives it means packets are dropped. If no. of dropped packets are more than threshold value (here 10) then leader nodes will send block message to all its neighbors. Block message contains id of malicious node. All intermediate nodes receives table having black hole node. Now, again new RREQ message is generated for route discovery.

The Working Flow of SCAODV Approach is shown in following figure 4**:**

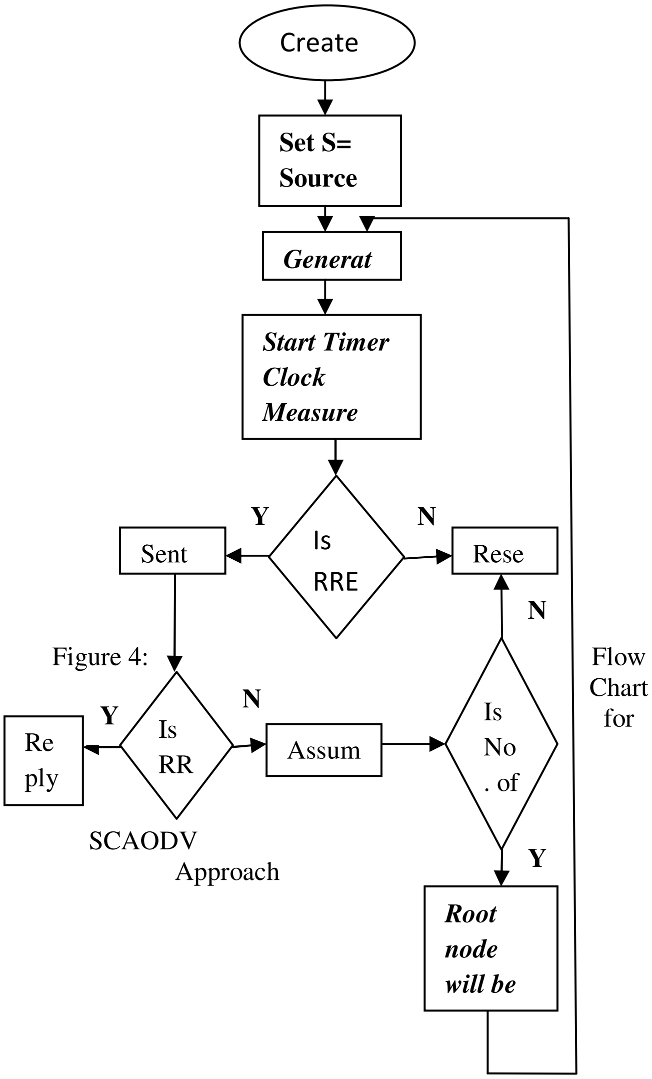


Figure 4: Flow Chart for SCAODV Approach

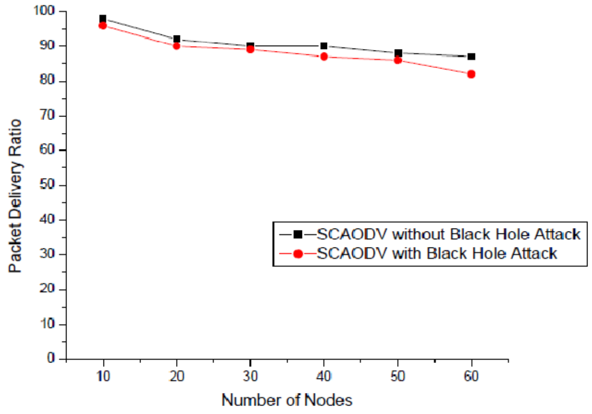
VI. Results and Discussion

Table: 7.1 shown the simulations settings used:

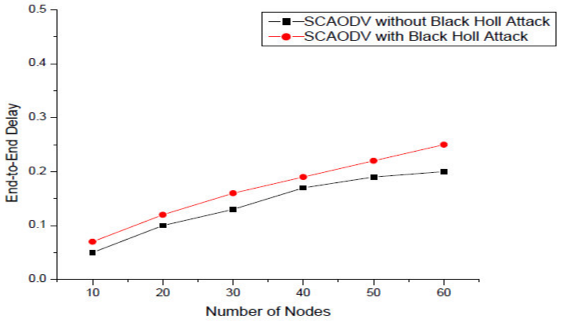
PARAMETERS	VALUES
Simulation time	600 seconds
Simulation area (m x m)	500 × 500
Number of Nodes	10 to 60
Transmit Power(W)	0-005
Packet size (bits)	1024 MB
Pause time	100 seconds
Performance Matrix	Packet Delivery Ratio, and End-to-end delay, Network throughput.
Mobility Speed	0 to 20 meter/second

In this simulation, first we observed the effect of the Packet Delivery Ratio (PDR) measured for the SCAODV protocol when the node mobility increases.

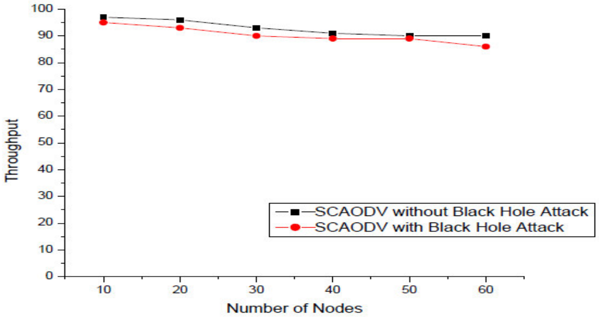
In Graph 1, it can be observed that packet delivery ratio in the network with/without black hole node decreases when the node speed increases. Moreover, the PDR is high in the network operating in normal condition compared to when the network operates in the presence of black hole attack is present. This is due to the presence of the malicious node which drops the packets when it receives them. Graph 2 shown End-to-End Delay performance and Graph 3: shown the throughput comparisons.



Graph 1: Packet Delivery Ratio vs. Number of Nodes

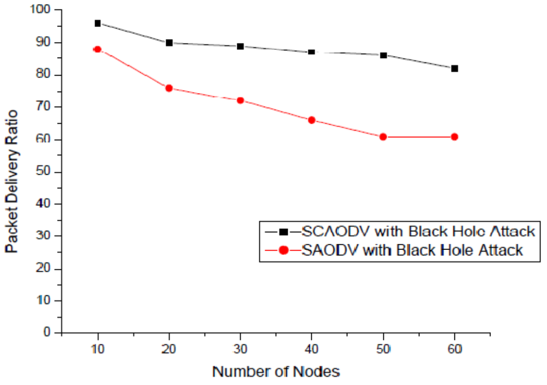


Graph 2: End-To-End Delay Vs. Number of Nodes.

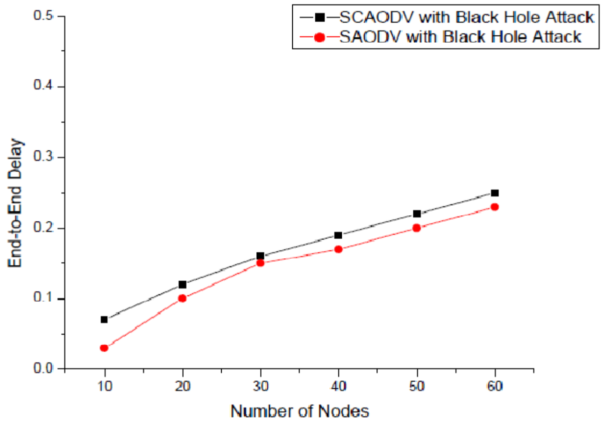


Graph 3: Throughput vs. Number of Nodes

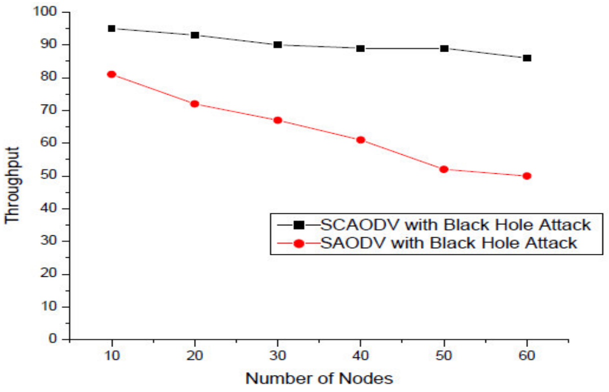
Now we compare the performances of SAODV and SCAODV protocols based on different parameters. The compression is shown on the following graph 4, graph 5 and graph 6.



Graph 4: Compression of SCAODV and SAODV (Packet Delivery Ratio vs Number of Nodes)



Graph 5: Compression of SCAODV and SAODV (End-to-End Delay vs Number of Nodes)



Graph 6: Compression of SCAODV and SAODV (Throughput vs Number of Nodes)

VI. Conclusion

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. The main goal of our thesis was to help improve the security in MANETs against collaborative black hole attacks. Firstly, we have analyzed the behavior and challenges of security threats in mobile ad hoc networks as well as how black hole attacks affect the performance and security for such networks. After some extensive research on many recent ideas of black hole attack prevention in MANETs, we were able to suggest ideas to address the problem of collaborative black hole attacks in MANETs.

Although many solutions have been proposed to mitigate the black hole attacks in MANETs, most of the solutions proposed were reactive in nature i.e. they can identify the malicious node only after the attack has been carried out by the malicious node. Many of these solutions are also only capable of mitigating single black hole attack and are not capable of avoiding collaborative black hole attack. For mitigation of black hole attack in MANETs, firstly, we proposed the SCAODV scheme, a feasible AODV based solution to mitigate black hole attacks in MANETs. We simulate our proposed solution using NS3 simulator and compare the performance with SAODV in terms Packet Delivery Ratio, Throughput and End-to-End Delay. Simulation result shown that the SCAODV performance is good as compare to SAODV. In future we have implemented this approach.

References

[1] [1].C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. /E€€ SlCON '97, Apr. 1997, pp. 197-211.

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91.

[3] Z. Karakehayov, “Using REWARD to Detect Team Black- Hole Attacks in Wireless Sensor Networks,” Wksp. Real-World Wireless Sensor Networks, June 20–21, 2005.

[4] S. Lee, B. Han, and M. Shin, “Robust Routing in Wireless Ad Hoc Networks,” 2002 Int’l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[5] Umesh Kumar Singh[1], Kailash Phuleria[1], Shailja Sharma[2]& D.N. Goswami[2], An analysis of Security Attacks found in Mobile Ad-hoc Network, International Journal of Advanced Research in Computer Science, Volume 5, No. 5, pp. 34-39, May-June 2014.

[6] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.

[7] Shuyao Yu, Youkun Zhang, Chuck Song and Kai Chen, security architecture for Mobile Ad Hoc Networks”. http://www.portal.prozhe118.com, pp.1-4.

[8] L. Peters, F. De Turck, I. Moerman, B. Dhoedt, P. Demeester, and A. A. Lazar, "Network layer

solutions for wireless shadow networks," Proceedings of the International Conference on networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, , vol. 2, 2006.

[9] S. A. Razak, S. M. Furnell, and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols," www.scm.tees.ac.uk, pp.-1-6, 2004.

[10] A. Mishra, Security and Quality of Service in Ad Hoc Wireless Networks, 2008.

[11] L. Tamilselvan and V. Sankaranarayanan, "Prevention of co-operative black hole attack in MANET," Journal of networks, vol. 3, pp. 13-20, 2008.

[12] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," IEEE Communications Magazine, vol. 40, pp. 70-75, 2002.

[13] S. Saraeian, F. Adibniya, M. GhasemZadeh, and S. Abtahi, "Performance Evaluation of AODV Protocol under DDoS Attacks in MANET," Proceedings of World Academy of Science, Engineering and Technology, vol. Vol. 33, pp. 501 - 503, September 2008.

[14] Abolhasan, M., Wysocki, T., and Dutkiewicz, E. A review of routing protocols for mobile ad hoc networks. Ad Hoc Networks, 2(1), 2004, pp. 1–22.

[15] Umesh Kumar Singh, Kailash Chandra Phuleriya, Shailja Sharma & D.N. Goswami, On Protocols to Prevent Black Hole Attacks in Mobile Ad Hoc Networks, nternational Journal of Electronics Communication and Computer Engineering, Volume 6, Issue 1, pp. 55-60, year-2015.