International Journal of Scientific Research in Computer Science & Engineering
Research Paper Volume-3, Issue-1 ISSN: 2320-7639

On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks

Umesh Kumar Singh[1]*, Jalaj Patidar[2] and Kailash Chandra Phuleriya[3]

[1*,2,3] School of Engineering & Technology, Vikram University, Ujjain (M.P.) India

Available online at www.isroset.org

Received: 04 Dec 2014 Revised: 20 Dec 2014 Accepted: 30 Jan 2015 Published: 28 Feb 2015

Abstract- Wireless or Mobile ad hoc Networks (MANETs) emerged to replace the wired networks. MANETs are extensively used in military and civilian applications. The wireless and dynamic nature of MANETs makes them more vulnerable to security attacks when compared with fixed networks. The existing routing protocols are optimized to perform the routing process without considering the security problems. In this paper, we have examined the effect of black holes attacks on the networks. We have also presented a protocol to identify multiple black holes collaborating with each other and a solution to determine a safe route to protect our network on cooperative black hole attack, while showing the future aspects.

Keywords: MANETs, Black Hole, Routing, SAODV, DSR

1. INTRODUCTION

In past few years, the explosive growth of mobile computing devices, which mainly include android cell phones, laptops, personal digital assistants (PDAs) and handheld digital devices, has encouraged a radical change in the computing world. With the emergence of ubiquitous computing research in wireless network is the need of the hour. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method as it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices [1].

A MANET is a collection of mobile nodes sharing a wireless channel without any centralized control or established communication backbone. MANET has dynamic topology and each mobile node has limited resources such as battery, processing power and onboard memory. MANETs were initially proposed for military applications and currently their use has been enlarged [2]. MANETs consist of mobile nodes, which can communicate with each other and nodes can enter and leave the network any time due to the short transmission range of MANETs, routes between nodes may consist of one or more hops. Thus each node may either work as a router or depend on some other node for routing [3]. Figure-1 shows a simple ad hoc network with three mobile hosts using wireless interfaces. Host A and C are out of range from each other's wireless transmitter. When exchanging packets, they may use the routing services of host B to forward packets since B is within the transmission range of both of them.

Corresponding Author: Dr. U K Singh

School of Engineering & Technology, Vikram University, Ujjain (M.P.) India

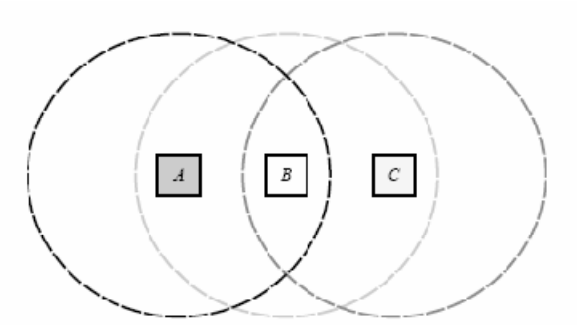


Figure- 1: Mobile Ad hoc network with three mobile nodes [4].

The rest of the paper is organized as follows. In section 2, we have presented the related works. In section 3, we have described a black hole attacks scenario. In section 4, we have examined in SAODV and DSR protocols in detail. Then in section 5 we have described simulation setup and scenarios, and compared the solutions. Finally, we concluded our study in section 6.

2. RELATED WORK

Recent research on MANET shows that the MANET has larger security issues than conventional networks and a lot of research has focused on the cooperation issues in MANET.

In [5], author proposed solutions to identify and eliminate a single black hole node. However, the case of multiple black hole nodes acting in coordination has not been addressed. In [6], authors present two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission. This technique is imperfect due to collisions, limited transmit power and partial dropping. In [7], author proposed the CORE scheme and various related issues in. According

Michiardi and Molva scheme, every node computes a reputation value for every neighbour, based on observations that are collected in the same way as watchdog. Deng et.al in [8] have discussed discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. However, this increases the routing overhead and end-to-end delay. In addition, the intermediate node needs to send RREP message twice for a single route request. Raj et.al in [9] discussed a protocol viz. DPRAODV (Dynamic, Prevention and Reactive AODV) to counter the Black hole attacks. In the simulation results, the packet delivery ratio is improved by 80-85% than AODV when under black hole attack, and 60% when traffic load increases. The advantage of DPRAODV is that it achieves an obviously higher packet delivery ratio than the original AODV. Thus, the protocol though successful, suffers from the overhead of updating threshold value at every time interval and generation of the ALARM packets. The routing overhead, as a result is higher.

There are three main routing protocols proposed for MANETs: Ad hoc on demand Distance Vector (AODV) [10] routing, Destination Sequence Distance Vector routing (DSDV) [11] and Dynamic Source Routing [DSR] [12]. AODV and DSR belong to on-demand routing protocols and DSDV is a table-driven routing protocol. DSR is completely on-demand ad hoc network routing protocol collected of two parts: Route Discovery and Route Maintenance. Here, the basic form of Route Discovery and Route maintenance in DSR is described. In DSR, when a node has a packet to send to some destination and does not currently have a route to that destination in its Route Cache, the node initiates Route Discovery to discover a route; this node is known as the initiator of the Route Discovery, and the destination of the packet is known as the Discovery's target. AODV stand for Ad-Hoc on Demand Distance Vector Protocol [13-14] and is, as the name already says, a reactive protocol, even though it still uses characteristics of a proactive protocol. It is reactive protocol, when a node wishes to start transmission with another node in the network to which it has no route; AODV will provide topology information for the node. AODV use control messages to find a route to the destination node in the network.

3. BLACK HOLE ATTACKS

In black hole attack a malicious node [15] may advertise a good path to a destination during routing process. The intention of the node may be to hinder the path finding process or interpret the packet being sent to destination. Alternatively black-hole scenario may be defined as the one in which the cannel properties tend to be asymmetric i.e. the signal strength in both direction may not be same. In this case a node which receives the data packet but does not forward it is termed as black hole. In either case the normal operation of the MANET is disrupted [16].
Figure-2 shows how black hole attack occurs. Node "KP" wants to send data packets to node "Dr. UKS" and start the route detection process. So, if node "LL" is a malicious node then it will claim that it has active route to the particular destination as soon as it receives route reply packets. It will then send the response to node "KP" before any other node. In this way node "KP" will think that this is the active route and thus active route detection is complete. Node "KP" will ignore all other responds and will start sending data packets to node "LL". In this way all the data packet will be lost consumed or lost.

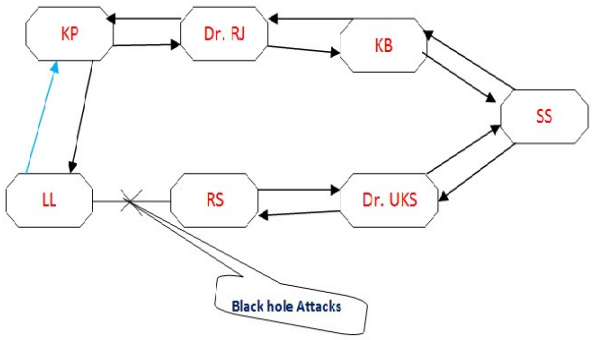


Figure-2: A black-hole attack scenario [3].

4. COOPERATIVE BLACK HOLE ATTACK PREVENTION PROTOCOLS

Basis of our study, in this section we compare the performances of Cooperative Black Hole Attack prevention protocols. Various researchers proposed several protocols to protect Black hole attach and provide safe communication and also provide reliability. So we select two protocols in our study: SAODV and DSR,

1. SAODV

(Secure Ad-Hoc on Demand Distance Vector): A secure version of AODV is called Secure AODV. The SAODV is a combination of two schemes for securing ADV. It provides features such as reliability, confirmation, and non- repudiation of routing data. It incorporates two schemes for securing AODV. To preserve the collaboration mechanism of AODV, SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the double signature: when a node A generates a RREQ message, in addition to the regular signature, it can include a second signature, which is computed on a fictitious RREP message towards A itself. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node A. If one of these nodes then receives a RREQ towards node A, it can reply on behalf of A with a RREP message, similarly to what happens with regular AODV. To do so, the intermediate node generates the RREP message, includes the signature of node A that it previously cached; and signs the message with its own private key. SAODV does

not require additional messages with respect to AODV. Nevertheless, SAODV messages are significantly bigger, mostly because of digital signatures.

2. DSR:

DSR stand for Dynamic Source Routing (DSR). The individual feature of DSR is the use of source routing. DSR is a reactive protocol i.e. it doesn't use periodic updates. It computes the routes when necessary and then maintains them. In DSR, each node uses cache technology to maintain route information of all the nodes. In the communication systems DSR used two stages these are; Route discovery and Route maintenance

When a source node wants to send a packet, it first consults its route cache. If the required route is available, the source node sends the packet along the path. Otherwise, the source node initiates a route discovery process by broadcasting route request packets. Receiving a route request packet, a node checks its route cache. If the node doesn't have routing information for the requested destination, it appends its own address to the route record field of the route request packet. Then, the request packet is forwarded to its neighbors. If the route request packet reaches the destination or an intermediate node has routing information to the destination, a route reply packet is generated. When the route reply packet is generated by the destination, it comprises addresses of nodes that have been traversed by the route request packet. Otherwise, the route reply packet comprises the addresses of nodes the route request packet has traversed concatenated with the route in the intermediate node's route cache. Whenever the data link layer detects a link disconnection, a Route Error packet is sent backward to the source in order to maintain the route information. After receiving the Route Error packet, the source node initiates another route discovery operation. Additionally, all routes containing the broken link should be removed from the route caches of the immediate nodes when the Route Error Packet is transmitted to the source. The advantage of this protocol is reduction of route discovery control overheads with the use of route cache and the disadvantage is the increasing size of packet header with route length due to source routing [17-19].

In this study some important routing protocols are considered which can be used to prevent black hole attacks in MANET. We have shown a comparative study using some parameters as shown in table-1;

Table - 1: Comparison of routing protocols under study

Routing Protocols	Update Destination	Update Period	Unidirectional Links	% to Prevent Black Hole Attack	Multiple Routes
SAODV	Source	Event Driven	Yes	90%	Yes
DSR	Source	Event Driven	No	79%	Yes

5. SIMULATION ENVIRONMENT

It is clear from the table-1 that no such protocols are proposed which provide a guarantee to prevent black hole protocols 100%. In this section we have compared the performance of these protocols using NS-2[2.29] network simulator [20]. Mobility scenarios are generated by using a random way point model by varying 10 to 50 nodes moving in simulation area of 700m x 700m. In this simulation study, we have used the following parameters: Table-2: Simulation Setting:

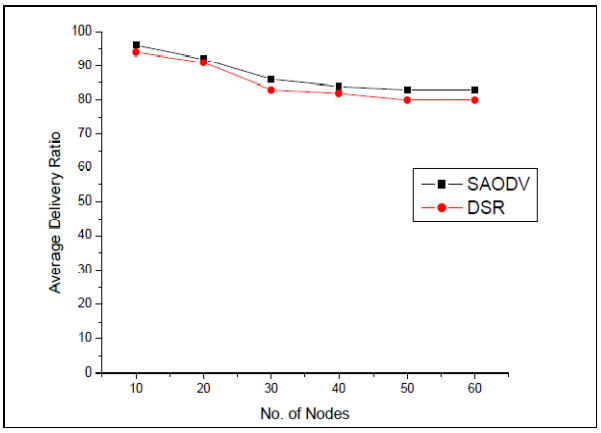
Parameter	Value
Simulation Time	500(s)
Number of Nodes	10 to 60
Mobility	10-50m/s
Routing Protocol	AODV, SAODV, DSR
Pause Time	10 (m/s)
Simulation Area	500 x 500m
Transmission Range	200m
No. Of Malicious	Node 1

The research community considers the following matrices in order to evaluate and compare the performance of energy conscious MAC protocols. This is mandatory for protocols in order to provide best support on real time application looking on to the great requirement of such protocols. In order to check the performance of the designed protocol we have given a matrix which is as follows [21].

- **Average Delivery Ratio:** The average packet delivery ratio is the number of packets received to the number of packets sent averaged overall the nodes.
- **Average End-to-End Delay:** This is the average delay between the sending of the data packet by the source and its corresponding receiver. It includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays in milliseconds.
- **Network Throughput:** The network throughput is defined as the total number of packets delivered at the sink node per time unit.

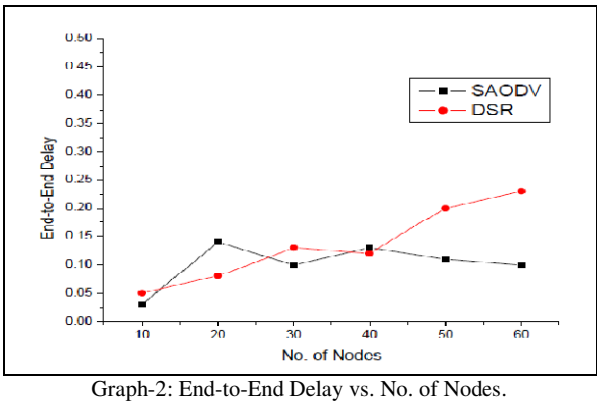
In the following graphs-1, 2 & 3, we have compared the performances of SAODV and DSR protocols.

In graph-1, we compared the performance of SAODV and DSR protocols with Packet Delivery Ratio (PDR) vs. No. of Nodes. It is observed that the SAODV protocols protect networks more effectively as compared to DSR and provide better Packet Delivery Ratio.



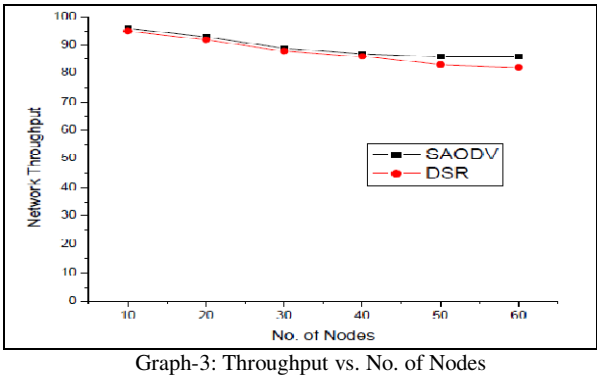
Graph-1: Packet Delivery Ratio vs. No. of Nodes

In graph-2, we compared the performance of SAODV and DSR protocols with End-to-End Delay vs. No. of Nodes. It is observed from this graph that the SAODV protocols performed minimum delay as compared to DSR.



Graph-2: End-to-End Delay vs. No. of Nodes.

Graph -3 shows that when a network suffers from black hole attack then the throughput of network is decreased. But as a compared to SAODV it provides better throughput.



Graph-3: Throughput vs. No. of Nodes

6. CONCLUSION

In this paper, we have studied the common problems related to black hole attacks in MANET routing. Further, we studies some important black hole prevention protocols and opted two protocols which are SAODV and DSR protocols for this study. We have provided the relative performance of SAODV and DSR protocols using network simulator. In this study we have observed that the SAODV protocol provides a better performance as compared to DSR. It shows that no such schemes are available to prevent black hole attacks without affecting the performances of network. In future we have planned to develop a new scheme for MANET to provide better performance as compared to other schemes available for this purpose.

REFERENCES

[1]. Umesh Kumar Singh, Kailash Phuleriya, Shailja Sharma, D.N. Goswami, A Comparative study of Collaborative Attacks on Mobile Ad-Hoc Networks, International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 8, pp.183-187, August 2014.

[2]. Umesh Kumar Singh, Lokesh Laddhani and Kailash Chandra Phuleriya, An Analysis of MANET Routing Protocols with Effective Resource Management, International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 6, pp. 724-729, June 2014.

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

[4]. Pooja Jaiswal and Dr. Rakesh Kumar, Prevention of Black Hole Attack in MANET, IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), Vol.2, No5, pp. 599-606, October 2012.

[5]. Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine,Vol.40, no.10, October 2002.

[6]. S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks. In mobile Computing and Networking (MOBICOM), pages 255–265, 2000.

[7]. P. Michiardi and R. Molva. Preventing denial of service and selfishness in adhoc networks. In Working Session on Security in Ad Hoc Networks, Lausanne, Switzerland, June 2002.

[8]. Deng H., Li W. and Agrawal, D. P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2002.

[9]. Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[10]. Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) routing," Internet Draft, November 2002.

[11]. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Computer Communications Review, pp. 234-244, October 1994.

[12]. D.Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, 2007.

[13]. Perkins C.E., Elizabeth M., Royer & Samir R., "Ad hoc On- Demand Distance Vector Routing, IEFT MANET Draft, Charles E. Perkins, Ad Hoc Networking, ISBN 0-201-30976-9, 2003.

[14]. Raja L., & Santhosh B., "Comparative study of reactive routing protocol (AODV, DSR, ABR and TORA) in MANET", International Journal of Engineering and Computer Science, Volume 2 Issue 3, PP. 707-718, 2013.

[15]. Bing Wu, Jianmin Chen, Jie Wu & Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, WIRELESS/MOBILE NETWORK SECURITY Y. Xiao, X. Shen, and D.-Z. Du (Eds.), Springer, pp. 1-38, 2006.

[16]. Nagpal C., Kumar C., Bhushan B. & Gupta S., A Study of Black Hole Attack on MANET Performance, I. J. Modern Education and Computer Science, pp. 47-53, 2012.

[17]. Manickam P. ,Baskar T &.Manimegalai D., "Performance Comparisons Of Routing Protocols In Mobile Ad Hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, pp. 98-106, 2011.

[18]. Johnson D. B., Maltz D. & Broch J., "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Network", C.E. Perkins, Ed., Addison-Wesley, pp.139-172, 2001.

[19]. Prateek K., Arvind N.& Alaria S., "MANET-Evaluation of DSDV, AODV andDSR Routing Protocol", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2 Issue 1, pp.-99-104, 2013.

[20]. The network simulator. (http://www.isi.edu/nsnam/ns/).

[21].Umesh Kumar Singh, Kailash Chandra Phuleriya and Rakhi Sunhare, Wireless Sensor Networks: Comparative Study and Analysis of MAC Protocols, International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), Vol. 4, Issue 2, pp. 107-114, Apr 2014.

.

