Prevention of Co-operative Black Hole Attack in MANET on DSR protocol using Trapping

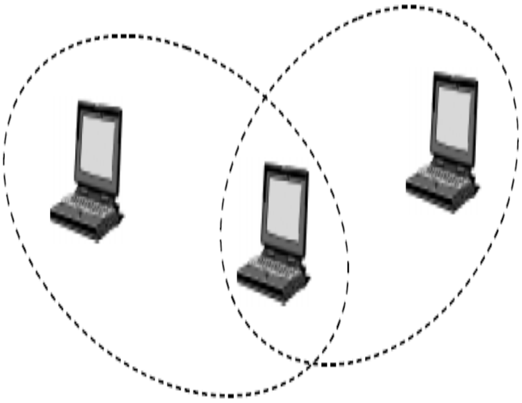
Sandeep Kumar, Er.Rupinder Kaur

***Abstract*— The Mobile ad-hoc network (MANET) is accumulation of wireless mobile connecting point at which several lines come together in which each node can put across with other node without use of predefined substructure and these system are utilized to set up a wireless communication in a modern environment without the use of any kind of predefined infrastructure. It is basically a temporary network set up by wireless nodes usually moving randomly and communicating without a network infrastructure. Due to the massive existing of mobile ad hoc network, presently a lot of efficient protocols have been aimed for MANET. All of these efficient Routing protocols are depends only strong belief and supportive environment. Conversely, the networks are more dangerous to various kinds of routing attacks with the presence of malicious nodes. Black hole attack is one of network layer attack. In this attack, A malicious node make use of routing protocol to call attention to itself that has a shortest path to reach destination, drops at the cost of original routing packets. In our work, the proposed algorithm is used to secure the DSR protocol. This will help to improve the performance of Mobile Ad hoc network due to the attack. There are several prevention mechanisms to eliminate the Black Hole attack in MANET. The aim of the paper is to provide better prevention of Co-operative Black Hole attack in MANET and how it affects the performance metrics in terms of throughput and delay of the network by comparing the network performance with and without black hole nodes.**

***Index Terms*— Mobile ad-hoc networks, DSR protocol, Black hole, Trap Header (TH).**

I. INTRODUCTION

Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes .Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks. Because these networks are temporary, they can be attacked from within, due to being constructed without protection, in poor conditions. Attacks are also launched if nodes are compromised. Another issue is the node number. Hundreds/thousands of nodes might be required in a network and security measures undertaken must be efficient and cost effective for a vast network. Exchange of topological information among nodes is facilitated by routing protocols to establish routes and this is used by attackers for acts including bogus routing, incorrect forwarding, lack of error messages, restricted reply time, thereby leading to retransmission and inefficient routing. Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. Common attacks faced by networks include black Hole, grey hole and wormhole attacks, and IP spoofing. Black hole attacks are harmful nodes that refuse to forward traffic.



. **Figure.1: Example of a Simple Ad-Hoc Network with three Participating nodes**

The outer most attacks can be prevented by using standard security scheme like a firewalls, encryption etc. And the Internal attacks are typically more severe attacks, since malicious insider nodes already belong to the network as an authorized party and are thus secured with the security mechanisms the network and its services offer. Thus such malicious insiders who may even operate in a group may use the standard security means to actually protect their attacks. These kind of harmful parties are called compromised nodes, as their actions compromise the security of the whole ad hoc network. Figure1. Shows a simple ad hoc network with three nodes .The outermost nodes are not within transmitter range with each other. However the middle node can be used to forward packets between the outermost nodes. The middle node acting like a router and the three nodes have formed an ad hoc network

Manuscript received April 24, 2015.

Sandeep kumar, M-tech student, ECE Department, R.I.E.T College, Phagwara, Punjab Technical University, Punjab, INDIA

Er.Rupinder kaur, Assistant Professor, ECE Department, R.I.E.T College, Phagwara, Punjab Technical University, Punjab, INDIA

II. RELATED WORK

D. Maltz Confronted a new protocol Ariadne (A Secure On Demand Routing Protocol for Ad Hoc networks) based on the DSR protocol for routing aegis. Several certification methods like digital signatures, MACs computed with pair-wise secret keys, or TESLA could be used with the proposed protocol. Hash chains are used to authenticate every route request protecting the network from overload, so denial of service attacks can be prevented. Attacks from settled nodes from tampering with the uncompromised nodes are also kept by the proposed method. Mixtures of TESLA authenticators (MACs) are added by intermediate routers and a hashing technique to protect the discovered routes. The proposed method's security mechanisms are effective and can also be used for wide variety of routing protocols. D. Jhonson examines the black hole attack and cooperative black hole attack which is one of the new and possible attacks in ad hoc networks. In this attack a malicious node exposing itself and shows the shortest path to the node whose packets it wants to intercept. To overcome the chances it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is known as cooperative black hole attack. In our research we find out a secure route between source and destination by identifying and isolating black hole nodes. In this paper, via simulation, the proposed solution are evaluated and compared it with standard DSR protocol in terms of throughput, Packet delivery ratio and latency.

III. METHODOLOGY

A) Dynamic Source Routing

It is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of *Route Discovery* and *Route Maintenance*, which work together to allow nodes to discover and maintain *source routes* to arbitrary destinations in the ad hoc network. The use of source routing allows packet routing to be trivially loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded, and allows nodes forwarding or overhearing packets to cache the routing information in them for their own future use. All aspects of the protocol operate entirely aspects of the protocol operate entirely *on-demand*, allowing the routing packet overhead of DSR to scale *automatically* to only that needed to react to changes in the routes currently in use.

B) Route Discovery

It is the method by which a node S wants to send a packet to a destination node D and obtains a source route to D .This is happened only when source ‘ S ‘ is trying to transmit a data packet to D.

C) Route Maintenance

It is the method in which node S is capable to detect, while using a source route to D, if the network topology has been changed so there is no longer use of its route to D because a link along the route no longer works. When Route Maintenance shows a source route is broken, then scan attempt to use any other route it happens to know to D, or it can invoke Route Discovery again to discover a new route for subsequent packets to D. Route Maintenance for this route is used only when S is actually transmitting packets to D.

D) Proposed modification in the DSR

In this paper the proposed routing is based on DSR with modification for detection of black hole attack. It is separated into two phases: Detection before route establishment and avoidance of harmful nodes during data forwarding. The salient advantages of this proposed method is its simplicity and effectiveness in detecting malicious nodes in dynamic scenarios. This algorithm has been designed based on the concept that malicious node may drop the packet or modify the packet. The DSR is modified to contain new header called Trap Header (TH). During the detection Time, the nodes firstly sources the entire two hop neighbor node id’s and send trap packets with TH consisting of incapacitate data destination to its two hop neighbors. And then if the receiving node states that it has the route to the invalid destination in its cache, and has forwarded the data packet to next hop then the node is assumed to be a black hole harmful node. This information about the maliciousness is stored in the nodes. During route discovery time, the nodes cross check the routes in it’s the node invalidates that route and starts a new and fresh route discovery avoiding the harmful node. Thus, the proposed method prevents the black hole attack by a simple method of trapping which is useful to detect the harmful nodes and avoiding it in any of the routes during transmitting data packets.

IV. RESULTS AND DISCUSSION

The proposed DSR is used for simulation to evaluate its performance and it is compared with the traditional DSR. The experiments are direct the course of varying speed of the mobile nodes. The speed is varied from 10 Km/h to 90 Km/h and produced the network performance. The black hole attack misbehavior is defined as either drop the packets or not to forward the packet in the giving time interval. DSR routing protocol parameters were set as shown in table 1.

Table 1:DSR Routing Parameters Used

Parameters	**Values**
Route expiry time	300second
Request Table size	64
Max. Transmission attempt	16
Time out value for non-propagating requests	0.03sseconds
Gratuitous route reply timer	1second
Maintenance hold off time during route maintenance	0.25 seconds
Maintenance acknowledgement time	0.5 seconds

Many performance metrics are used to compare the proposed DSR protocol with the existing one. The following metrics were considered for the comparison.

Packet Delivery Ratio (PDR): It is known as the ratio of the number of packets received and the number of packets sent.

Average End to End delay: It shows the mean time (in seconds) which is consumed by the packets to reach their paired destination ends. Table 2(a, b and c) tabulates the Number of hops to destination, end to end delay and packet delivery ratio obtained for the proposed DSR and DSR. Figure 2 to Figure 4 shows the same.

Table 2:Results of the experiments

Table 2(a):Values of no. of hops to destination

Mobility	No of hops to destination	
	DSR	Proposed DSR
10 Kmph	2.7	2.9
30 Kmph	3.2	3.6
50Kmph	3.5	3.8
70 Kmph	3.9	4.1
90 Kmph	4.2	4.4

Table 2(b):Values of end to end delay

Mobility	End to End Delay	
	DSR	Proposed DSR
10 Kmph	0.0514	0.0464
30 Kmph	0.0608	0.0582
50Kmph	0.0684	0.0618
70 Kmph	0.0726	0.0638
90 Kmph	0.0784	0.0692

It is cleared that the number of hops of the proposed DSR is slightly more than the previous DSR as shown in figure 2. This is due to avoiding the harmful nodes in the network, while sending data packets to the destination end. As the increase is negligible, when compared to DSR, the increase can be ignored.

Table 2(c):Values of packet delivery ratio

Mobility	Packet delivery ratio (PDR)	
	DSR	Proposed DSR
10 Kmph	0.9278	0.9432
30 Kmph	0.9148	0.9326
50Kmph	0.8842	0.9014
70 Kmph	0.8621	0.8942
90 Kmph	0.8544	0.8824

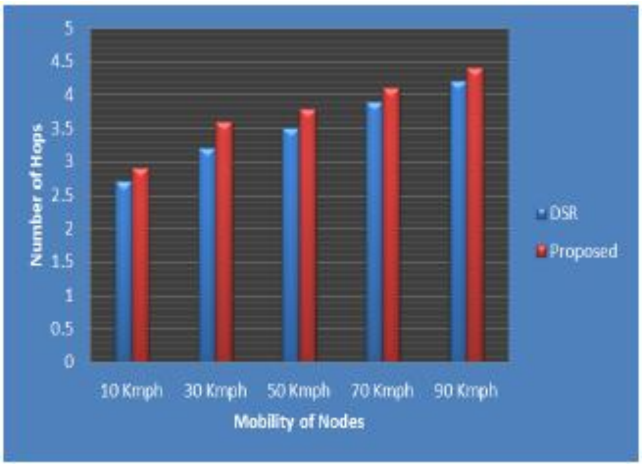


Figure 2.Numer of hops to destination

The end to end delay in the proposed DSR is low and it is observed that with the increase in number of nodes, the delay in DSR increases by 13.3%. Though, the number of hops from the source to destination increases, the end to end delay is less in the proposed DSR as shown in fig 3.

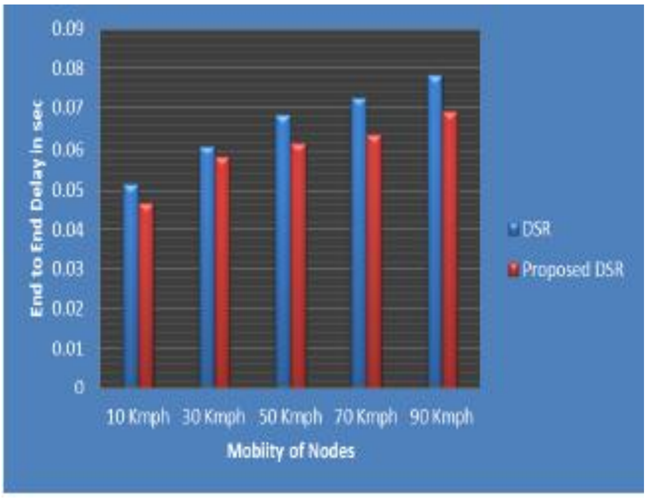


Figure 3.End to End Delay

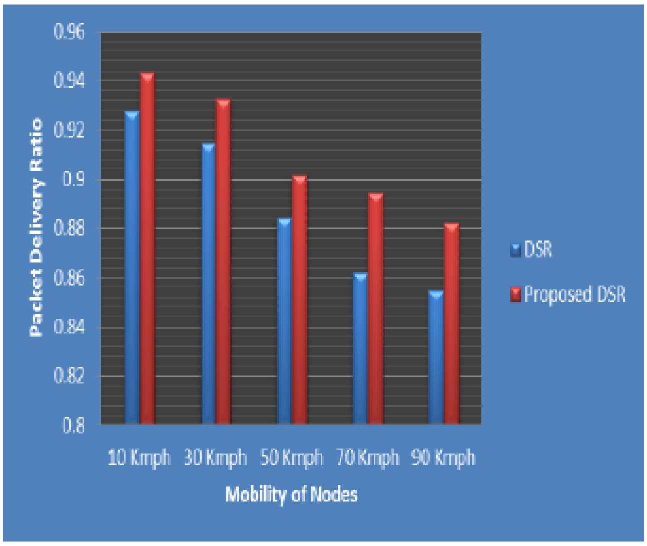


Figure 4.Paket delivery ratio.

The PDR improves with the use of modified DSR in the range of 1.57 % to 3.28% as shown in figure 4. It is observed from the tables and figures that the proposed DSR performance better than DSR in the presence of black hole attack.

V. CONCLUSION

Wireless mobile Ad Hoc network is likely to be attacked by the black hole attack. To solve this problem, a course based method is presented to detect black hole attack. The proposed solution is simulated using ns-2 and compared the modified DSR with original DSR in terms of throughput, end to end delay and network energy. Simulation results show that the proposed method has good performance against Black hole attack without much overhead. In the future, the DSR routing is modified to include a Trap Header to identify malicious nodes and the work may extend to propose a feasible solution which will strengthen original DSR against different types of attacks as warm hole attack and grey hole attack.

REFERENCES

[1] Zhao, Z., Hu, H., Ahn, G. J., and Wu, R. Risk-aware response for mitigating MANET routing attacks. IEEE Conference In Global Telecommunications (GLOBECOM 2010), December 2010, pp. 1-6.

[2] Mohapatra, P., Li, J., and Gui, C. QOS in Mobile Ad hoc Networks. IEEE Wireless Communications, June 2003, 10(3), pp. 44-52.

[3] Buchegger, S., Boudec, J.-Y.L. Nodes bearing grudges: Towards routing security, fairness, and robustness in Mobile ad hoc networks. [4] Al –Shurman M, Yoo S-M, Parks S, “Black Hole Attack in Mobile Ad Hoc Networks”, 42nd *Annual ACM Southeast Regional Conference (ACM-SE’ 42)*, Huntsville, Alabama, 2-3 April 2004.

[5] I.F. Akyildiz; X. Wang A Survey on Wireless Mesh Networks IEEE Communications Magazine, 43 (9), 23-30, (2005).

[6] Tamilselvan, L. and Sankaranarayanan, V., “Prevention of Blackhole attack in MANET”, *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications*. Aus Wireless, 21-21, 2007.

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

[8] Chang Wu Yu, Wu T-K Chang, “A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network”, *Emerging Technologies in Knowledge discovery and Data Mining*, Vol, 4819, Issue 3, 2007.

[9] Raja Mahmood RA, Khan AI. “A Survey on Detecting Black Hole Attack in AODV-based Mobile Ad Hoc Networks”. International Symposium on High Capacity Optical Networks and Enabling Technologies, Dubai, United Arab Emirates, 18-20 November 2007.

[10] Djenouri D, Badache N, “ Struggling Against Selfishness and Black Hole Attacks in MANETs”, *Wireless Communication and Mobile Computing* Vol. 8 Issue 6, pp 689-704, August 2008.

[11] H.Weerasinghe H. Fu., “Preventing Cooperative Blackhole Attack in Mobile Ad Hoc Networks, Simulation, Implementation and Evaluation”. *International Journal of Software Engineering and Its Application* vol.2, No.3, 2008.

[12] B. Wu, J. Chen, J. Wu, and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks," in Wireless/Mobile Network Security, *Springer* 2008.

[13] D.M. Shila; T. Anjali; “Defending selective forwarding attacks in WMNs, IEEE International Conference on Electro/Information Technology”, 96-101,2008.

[14] J.W. Cai; P. Yi, Y. Tian, Y.K. Zhou, N. Liu, “The Simulation and Comparison of Routing Attacks on DSR Protocol”, WiCOM 2009, in press.

[15] Kozoma W, Lazos L, “REAct: Resource- Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits”. *Second ACM Conference on Wireless Network Security*, 16-18 March 2009.

[16] Raj PN, Swadas PB, “DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET”, *International journal of Computer Science* Issue, Vol, 2 pp 54-59, 2009.

BIO DATA FOR AUTHORS

Mr.Sandeep Kumar received the B-Tech(bachelor of Technology degree in electronics and communication engineering)from the Ramgarhia institute of engineering and technology, Phagwara , under the Punjab Technical University ,in 2009.He is working as a lecturer in ECE department in Ramgarhia Polytechnic College , Phagwara since 2011.He is currently pursuing the M-Tech(part time)in the electronics and communication from the Ramgarhia institute of engineering and technology, phagwara under the Punjab Technical University.

Contact-00918427003552

Miss Rupinder Kaur received the B-Tech(bachelor of Technology in electronics and communication engineering)from the Sant Baba Bhag Singh institute of engineering and technology under the Punjab Technical University, in 2009.She has completed her M-Tech in ECE (Regular-full time) from the Lovely Professional University , in 2013. She has done her Thesis on Iterative decoding of Turbo codes. She got two years work experience as a Executive Engineer in the Indus Towers pvt ltd. In the year of 2009-2011.Currently she is working as a Assistant professor in ECE department in Ramgarhia institute of engineering and technology Phagwara since 2013.

Contact -00918968178179