© 2017 IJSRST | Volume 3 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Novel Study of Blackhole Attacks in MANET

Muntaha Manzoor Khan, Dr. Rakesh Kumar, Er. Preety Chaudhary
Sachdeva Engineering College for Girls, Gharuan, Mohali, Punjab, India

ABSTRACT

Mobile ad hoc network is used in all types of digital and data communication. Since it is wireless so it is more prone to attacks then other methods of communication. Actually it is decentralized system which means it uses autonomous wireless nodes. So every node can behave as a router as well as a host. Also the topology can be varied as nodes are mobile. These nodes have the self configuration policy so any other node can join the network and can influence the network. There are different types of attacks in MANET. In the network layer wormhole, blackhole, Byzantine and other attacks can occur. In this paper there is review of blackhole problem in the MANET.

General Terms
Wireless Communication, Network, Security Attacks, Nodes

Keywords
MANET, Blackhole, Mobile, routing.

I. INTRODUCTION

To protect the network efficient routing protocols should be used so that they can detect malicious node and can take detection and prevention measure to protect security. Worldwide many authors have worked in this area. Here is a complete review of work done in the area of blackhole attack in the MANET.

II. LITERATURE REVIEW

F. H. Tseng et al. [1] reviewed the prevailing provisions and also reviewed the modern methods used for routing. Authors classified the Blackhole attack and produced a comparative study on the basis of which a table was designed based on the analysis of these attacks.

Authors used the different assessment metrics of other routing protocol. It contains packet delivery ratio that is proportion (PDR), mobility variance with sum of errors, packet routing overhead, end-to-end delay by modifying in junction density [1].

Authors observed that the two proactive routing and reactive routing have advanced proficiency but suffered from different problems. The proactive detection technique had the good packet delivery proportion and correct diagnosis expectation, but deteriorated from the greater routing overhead as to the systeatically broadcast packets. The reactive diagnosis technique eliminated the routing overhead issue from the event-driven passage, but deteriorated from a few packet fall in the initial stage of routing method.

So to avoid all types of problems authors prescribed that a combined diagnosis method that had mixed benefits of proactive routing with reactive routing is the habit to upcoming investiation order. But they also urged that the striker's disorderly conduct was also can be the prime factor. The strikers could be talented to diagnose procedure, no circumstances what classes of routing diagnosis methods used. So solution of this problem can be use of few key encryption techniques or hash-based techniques.

N. Sharma et al. [2] analyzed the Blackhole attack in MANET and its solutions. Authors conveyed two possible outcomes. The initial one was to search alternatives than one route to the target or destination. The other was to utilize the packet order digit added in any packet header.

An arbitrary mesh was designed for the simulation reason and then checked for a group of parameters. We investigate proposed prototype for 50 nodes. Waiting time is changed from 0 to 900 sec. individual mobile junction in the MANET is promoted an initial rank inside the simulation boundaries (1000×1000) meters and handshakes the mesh at an arbitrary time. The packets are produced using CBR with rate of 4 packets per sec. The simulation or execution happens for 900 seconds every run. Junctions are usually scattered when initialized, and the starting location for the junction is described in a grouping structure file created for the simulation using an attribute within ns-2. The junctions proceed in erratic way between the simulation areas. Authors simulated for different solutions 1 and 2 with respect to the base protocol AODV. As for both conditions there was no striker node so authors tried to search the passage to the final location or target and leave the plea if it could not search the route.

Computer simulation showed that in comparison to the actual ad hoc on demand distance vector (AODV) routing strategy, the second alternative could search 75% to 98% of the route to the target based on the pause time at a minimum value of the delay in the meshes.

K. J. Sarma et al. [3] conducted a survey on Blackhole attack detection in MANET. The diagnosis methods that made utilization of proactive routing protocol had good packet delivery proportion and correct diagnosis expectation, but had greater overheads. The diagnosis methods that made utilization of reactive routing protocols have small overheads, but had greater packet drop issue. Depending on the over said execution correlations, it could be found that Blackhole strikers affect mesh contrary. So, there was requirement for ideal diagnosis and termination methods. The diagnosis of Blackholes in ad hoc meshes was still supposed to be a difficult task. Succeeding task was desired to an reliable Blackhole strike diagnosis and termination techniques with very low delay and overheads that could be utilized for ad hoc meshes vulnerable to Blackhole strikes.

D. R. Choudhury et al. [4] analyzed the MANET's routing protocol and refine the protection of viz. the Ad hoc On Demand Distance Vector (AODV) routing protocol. Authors proposed alterations to the AODV protocol utilized in MANET a methodology to overcome the Blackhole strike on the routing protocols in MANETs. Pause time and Request Reply Tab table designed to challenge the Blackhole strikes and the AODV protocol.

In the proposed algorithm authors initialized M_WAIT_TIME to be fifty percent of the cost of RREP_WAIT_TIME the time for which source junction hangs result, the source junction succeeding in getting initial RREP control report hangs for M_WAIT_TIME which was the sum of RREP time or 50% of it. For this interval, the RREP control messages prior to modifying RREQ. In over said solution, for this time, the source junction would retain whole the approaching RREP control reports in RREP_ Tab table.

The benefit of altering AODV protocol is that the infected junction was recognized at the earliest itself and there after eliminated so that it cannot participate in ongoing procedure. With no delay the malicious node were easily identified for further process, i.e. as we said before all the routes had unique sequence number. With no postponement of the infected junction were comfortably recognized i.e. as we termed before whole the routes had different order rank. Once, this type infected junction was recognized, suggested methodology adopted a solution having highest target order number from RREP_ Tab table. It did so, by calling over said own technique that is Pre_Receive Reply () technique.

To evaluate the packet delivery proportion, End-to-End Delay and Normalized Routing Overhead; execution was performed with junctions with the source junction transmitting at most 1000 packets to the target junction. It was checked from the evaluated graphs that PDR of AODV drops by 60.867 % in case of Blackhole strikes. The similar was gained by 60.877 % when proposed methodology was utilized in existing of the strike. At the same instant, results demonstrated that the increase in throughput is 13.28 %, demonstrated the throughput for before and upgraded was lacking than succeeding strike.

A Dhaka et al. [5] suggested a methodology in which a control order was sent to the adjacent junctions and wait expecting the junction replies. Depending on junction reply authors were capable to recognize the infected junction. The proposed method worked as if there was huge gap amid the Cseq of source junction and Rseq of nearby or central junction who had moved backwards Rseq or not. Usually the initial route responds would be from the infected junction with greater target order number which reserved in the initial position of Cseq-Table. Then differentiate the target Rseq with the Cseq in the table.

According to authors the benefits of over said procedure was that the infected junctions were recognized at the starting position itself and sharply terminated so that it could not involve in upcoming procedure. With junction laid the infected junction was easily recognized therefore authors said before whole the routes had different sequence number. Usually the infected junction had the large target order number and it was the initial Rseq to reach. So the contrast was done only to the initial participation in the table without modifying different participations in the table. [5]

The theoretical evaluation demonstrated that proposed methodology would sufficiently rise PDR with very small difference in routing overhead. The technique was uniformly implementable to different reactive protocols.

A. V. Kumar et al. [6] initiated to recognizing the bad performed nodes and removing them from the packet communications in different-hop mobile ad hoc meshes. The productive and well organized Audit Misbehavior Diagnosis and Monitoring Technique (AMDMM). It was successfully detected the all endless and particular packet droppers to lead the packets over the reputed junctions. In this over said research, the AMDMM integrated an description of bad performance nodes and also the report administration and trustworthy path searching positioned on the observable audits.

This structure be expressed by the three dominant aspects such as reputation, route discovery, and an audit monitoring development. These aspects communicated with operations of misbehavior, discovery of trustworthy paths and also the assessment of the credit amid the mobile junctions. This integrated structure was important for organizing credit among the junctions and it was completely established on the proposals of the audit monitoring procedure. In over said technique, individual junction had its personal view of the different junctions. The original and secondary hand instructions were taken into the examination for the assessment metrics. The original data managed the straight forward reviews of the junctions and the second hand data expressed the assumption of the different junctions. These two conclusions were utilized to recognize the reputation and misbehaving junctions in the complete mesh.

This over said prototype was executed using NS2 execution software. In this estimation the upcoming 10, 20, 30, and 40 group of mobile junctions are in different way dispersed in an environment. Individual junction had three positions in the physical environment, and arbitrary travels amid these neighborhoods with a constant speed. Authors utilized two way ground propagation prototypes. The antenna type was Omni antenna structure and the communication strength is 250m. Also, the utilized traffic variant is CBR and the AODV protocol is utilized for packet moving. In individual period, the source directed 10,000 packets to the target via the transmitted route. To segregate the execution deterioration due to infected dropping, minor, there might be the struggle and communications due to encounters were abstracted.

The AMDMM figured out junction attitude on a per-packet basis, beyond operating energy valuable overhearing methods or accelerated acknowledgment methods.

Md. A. Abdelshafy et al. [7] introduced a unique theory of Self-Protocol Trustiness (SPT) in which diagnosing an infected intruder was concluded by observing with the simple protocol attitude and attracts the malicious junction to give a latent confession of its malicious performance. Authors commenced a Blackhole Resisting Mechanism (BRM) to maintain such strikes that can be integrated into any reactive routing protocol. It did not lack costly cryptography or verification methods, but builds on section wisely enforced timers and brinks to organize junctions as nasty. No adjustments to the packet formats were demanded, so the overhead was a small chunk of computation at junctions, and no extra coordination.

Authors recommended a small up gradation to the original AODV by accumulating the previous three per hop times for a RREP obtained for a target. The average hop time was checked as the latency amid transmitting a RREQ and obtaining its correlating RREP parted by the hop count cost comprised in the RREP. Individual junction in the mesh had to check the performance of its nearby residents to diagnose if any misbehave as blackholes. BRM-AODV had no limits, such as RREP proportion, that might be calculated to infected junctions and recommended a passage for these infected junctions to perform under these limits.

The simulation outcome demonstrated that while the blackhole strike had numerous blow on the PDR of AODV specially for enormous amount of infected junctions, BRM-AODV accomplished an approximately regular PDF regardless the total number of infected nodes. On the other hand, while SAODV had a stable

PDR disregarding the number of infected junctions such as over said technique; it had a large PDR cost than SAODV.

S. R. Deshmukh et al. [8] proposed an AODV-based secure routing technique to diagnose and eradicate Blackhole strike and affected paths in the early interval of route search. A possible cost was attached with RREP which promises that there was no strike onward the path.

In ratio to the over said technique, a validity cost was set with the RREP header and is set in route table at individual junction of active passage. Whenever a junction gets route request, if it was the desired target or had a legitimate route, then route sending report will be displayed by setting cost for authentic bit in RREP. This RREP then will be moved previously to its nearby hop from which it obtained RREQ. The over said route reply report varies in the validity cost with the basic AODV route reply report. The validity cost strategy was applied in the RREP header. RREP of AODV would contain a secondary header digit in as potency digit.

In the primary AODV protocol, route table consisted of upcoming nine fields. In spite of these nine fields authors proposed an supplementary field for reliability cost. This recent field would be utilized to verify reliability of route. Authors concluded that with the growth in the number of junctions in the mesh originates packet delivery proportion to fall finally. In existence of striker junction in the mesh, there was a notable cut in PDR. But this junction could be halted from involving in the mesh using over said protocol which has PDR approximately same.

B. Sun et al. [9] presented a simple methodology for diagnosing black-hole strikes in movable ad hoc meshes, which, on being account of their mobility and being broadcast in character, were remarkably unprotected to strikes nearly equal to older wired meshes. In unique, black-hole strikes can be easily established by an conflict. To secure against this strike, authors devised a nearby residents-based technique to diagnose whether a Blackhole strike prevails and a routing recovery protocol to structure a good path to the true target. These techniques had the notable gain that the figure of encryption/decryption functions for checking was much low compared to those techniques overall depending on cryptography-based checking, thus saving maximum prototype resources (e.g. lowering energy consumption). Through simulation, authors evaluated these methods in terms of packet throughput, routing control overhead, detection probability, false positive probability and false negative probability. Simulation outcomes showed that techniques can effectively diagnose Blackhole strikes in the sense that diagnosing expectation (the probability that one attacker might be detected) in most cases is above 93%. At the same time, it did not reflect considerable routing control overhead. With the routing recovery technique, the packet throughput could be enhanced upto minimum 15% and the false positive expectation of the diagnosis theory is very small (less than 1.7%).

V. Kumar et al. [10] conveyed an increased efficient solution for diagnosing a Blackhole strike with small communication value in the MANET, which is usually easily prone to attack as compared to infrastructure-based meshes on account of its mobility and shared broadcast complexion. As a competitor could be strongly expand Blackhole strike in the mesh. It could be notice that over said work was extra secured than the present solutions. Authors also related its achievement to normal AODV routing protocol.

The over said outcome was an up gradation of standard AODV routing protocol, which would be capable to diagnose a Blackhole junction in the mesh. In over said algorithm, an approaching route reply table (CRRT) joined at the source junction. A CRRT collected the RREP packet, which holds knowledge about target order number, coming hop, hop figure, initial IP address, target IP address and lifespan. A source (S) junction wanted to talk with target (D) junction, they broadcast path request (RREQ) packet in the complete mesh.

Source (S) junction should use the over said (Th) cost to check the selected target order number of feedback junction. If the target order digit was greater than or equal to calculated threshold cost, it was known as Blackhole junction. Any other way, it was legitimate junction and it creates a route to target junction using above said target order rank. The over said technique presented superior achievement and more accuracy for diagnosing a Blackhole strikes in MANETs.

It was calculated that Packet Delivery proportion of normal AODV was greatly fall by 94.1 % when there was Blackhole junctions in the mesh, but Packet delivery proportion gains by 96.3 % when over said algorithm was utilized in the existence of a Blackhole junction.

It was measured that PDR drops by 95.2 in the presence of a Blackhole junction in the mesh, but over said technique increases it nearly 97.4.

It was calculated that Throughput of normal AODV was greatly fall nearly 310.13 kbps when there was a Blackhole junction in the mesh, but Throughput nearby gains by 333.9 kbps when over said technique is utilized was the existence of a Blackhole junction. The response to Throughput of normal AODV protocol, when counting of junctions was differing in the mesh.

It was calculated that Throughput of normal AODV falls nearly to 314.32 kbps in the presence of Blackhole junction in the mesh or network, and mean while Throughput gains nearly 336.14 kbps when over said supposed techniques utilized in the occurrence of a Blackhole junction.

Table 1: Comparison of Various Black Hole Attack Detection Solutions

Papers	Routing Type	Tool Used	Detection Type	Publication Year	Results	Defects	Resource
A survey of Blackhole attacks in wireless mobile ad hoc networks	Proactive (DSDV) and Reactive (AODV)	NS2	Cooperative Detection	2011	Detailed Study was provided and hybrid methodology is advised to use	Not proper methodology was addressed	Springer Journal-Human-centric Computing and Information Sciences
The Black-hole node attack in MANET	AODV	NS2	Single Detection	2012	Two solutions are provided	Efficiency	2nd IEEE Int'l Conference on ACCT
Implementing and improving performance of AODV by receive reply method and securing it from Blackhole attack	AODV	NS2	Single Detection	2015	Efficient and robust algorithm	Only capable of single malicious node detection	Elsevier- Int'l Conference on ACTA
Gray and Blackhole Attack Identi?cation using Control Packets in MANETs	AODV	NS2	Single Detection	2015	Malicious node is identified at beginning and is removed as earliest	Algorithm is based on hypothetical assumption that malicious node has highest destination sequence ID	Elsevier- 11th Int'l Conference on IMCIP
Reputed Packet Delivery using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks	AODV	NS2	Single as well as Cooperative Detection	2015	can detect selective dropping attacks over end-toend encrypted traffic streams	Robustness and efficiency is not discussed	Elsevier- Int'l Conference on ICCC
Resisting Blackhole Attacks on MANETs	AODV	NS2	Cooperative Detection	2016	Throughput is better	Power consumption and robustness is not discussed	13th IEEE Conference on CCNC
AODV-Based Secure Routing Against Blackhole Attack in MANET	AODV	NS2	Single as well as Cooperative Detection	2016	Algorithm works fairly good	Power consumption and robustness is not discussed	IEEE Int'l Conf. on RTEICT

III. CONCLUSION

In this review paper all types of Blackhole problems are discussed and also the solutions provided by different authors are summarized. Blackhole suffers from different problems like routing strategy, encryption strategy etc. So a proper mechanism should be used to avoid Blackhole problem in MANETs. In the future work more research papers can be studied to enhance the results of new algorithms.

IV. REFERENCES

[1]. F. H. Tseng, L. D. Chou, H. C. Chao, "A survey of Blackhole attacks in wireless mobile ad hoc networks," Springer Human-centric Computing and Information Sciences, pp. 1- 16, 2011.

[2]. N. Sharma and A. Sharma, "The Black-hole node attack in MANET," Second International Conference on Advanced Computing & Communication Technologies, pp. 546- 550, 2012.

[3]. K. J. Sarma, R. Sharma and R. Das, "A Survey of Blackhole Attack Detection in MANET," Internationai Conference on Issues and Challenges in Intelligent Computing Techniques, pp. 201-205, 2014.

[4]. D. R. Choudhury, L. Ragha and N. Marathe, "Implementing and improving the performance of AODV by receive reply method and securing it from Blackhole attack," International Conference on Advanced Computing Technologies and Applications, pp. 564- 570, 2015.

[5]. A. Dhaka, A. Nandal and R. S. Dhaka, "Gray and Blackhole Attack Identification using Control Packets in MANETs," Eleventh International Multi-Conference on Information Processing, pp. 83- 91, 2015.

[6]. A. V. Kumar, K. Selvamani and P. K. Arya, "Reputed Packet Delivery using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks," International Conference on Intelligent Computing, Communication & Convergence, pp. 489- 496, 2015.

[7]. Md. A. Abdelshafy, P. J. B. King, "Resisting Blackhole Attacks on MANETs," 13th IEEE Annual Consumer Communications & Networking Conference, 2016.

[8]. S. R. Deshmukh, P. N. Chatur and N. B. Bhople," AODV-Based Secure Routing Against Blackhole Attack in MANET," IEEE International Conference On Recent Trends In Electronics Information Communication Technology, pp. 1960- 1964, 2016.

[9]. B. Sun, Y. Guan and J. Chen, "Detecting black-hole attack in mobile ad hoc networks," Personal Mobile Communications Conference, 2003. 5th European, 2003.

[10]. V. Kumar and R. Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network," Elsevier ICCC- 15, pp. 472- 479, 2015