International
Journal
Of Advanced Research in Engineering & Management (IJAREM)
ISSN: 2456-2033 || PP. 52-57

Resolving Black Hole attack in Integrated Internet MANET

SHAISTA MEHDI KHATOON, WAJEEHA FAROOQ RUMI, TAHERA BANU, C ATHEEQ
DCET

Abstract: The integration of internet and MANETs offers ascend to heterogeneous system where viable correspondence between a fixednode in a web and a mobile node in a MANETs is a challenging task. This integration increases the application domain of MNAETs. However gateways are utilized for correspondence between them. The information going in heterogeneous system must be shielded from various types of attacks. The blackhole attack is one of the notable security dangers in integrated internet MANET. In order to provide communication in IIM, the mobile nodes have to first discover the gateway as it is important and inescapable and for this purpose the intruders utilizes the loophole to carry out their malicious behaviors. We propose an algorithm that detects and resolves the black hole attack. Simulation results show that our work is better than existing in terms of security deployment.
Keywords: integrated internet MANET, trusted table, trust, promiscuous mode.

1. Introduction

A Mobile Ad hoc Network (MANET) [1] is an infrastructure less wireless system. A MANET is made out of stations that speak with each other specifically in a shared manner. In this way, an ad hoc network is free of any current system framework, for example, base stations and access points. Although an autonomous, stand-alone Integrated Internet MANET

MANET is useful in many cases, a MANET associated with the Internet is substantially more alluring. This is on account of Internet assumes an imperative part in the day by day life of numerous individuals by offering a wide scope of administrations. This system interconnection between a MANET and the wired internet is accomplished by utilizing gateways and ad hoc routing that is required to route packets inside a MANET, as well as from a MANET to the Internet. The integrated internet and MANET is represented in fig 1.

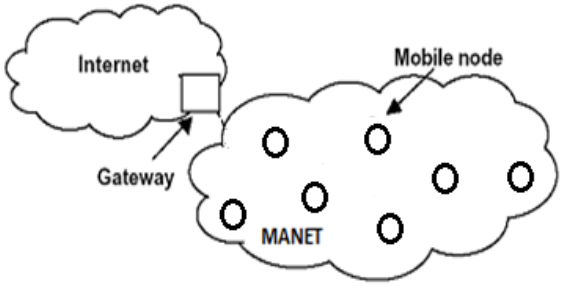

Fig.1 Integrated Internet-MANET

The ad hoc routing protocols proposed for MANETs are the promising routing protocols and can be used to routing packets between mobile nodes. Collaboration between mobile devices provides multi-hop communication among themselves. In any case, they can't give Internet access to the mobile devices since they don't bolster routing between a settled system like the Internet and a portable hub in MANET. In the Internet draft "Worldwide Connectivity for IPv6 Mobile Ad Hoc Networks"3 an answer is exhibited where the one of the MANETs steering protocol(AODV) is modified in a manner that it can route packets inside a versatile MANET, as well as to an wired system, yet it is not considering security mechanism.

The security dangers have been broadly talked about and explored in the wired and wireless networks, the correspondingly puzzling circumstance has additionally happened in MANET because of the inalienable outline abandons. There are numerous security issues which have been considered as of late. For example,

snooping attack, wormhole attack, black hole attack, routing table overflow and poisoning attack, packet replication, denial of service (DOS) attack, distributed DOS (DDOS) attack and so forth. Particularly, the bad conduct routing issue is one of the promoted security threat, for example, black hole attacks. A few scientists propose their protected routing thought to explain this issue, yet the security issue is still not able to avoid totally.

The primary challenge here stems from the need of selecting a trusted mobile node in MANET for secure information transmission in the field of integrating internet with MANET. Along these lines, a viable trusted component is required for this environment in such a case, the mobile node needs to choose which one of its neighbor dependable node is the ideal one for its correspondence. Investigating and tending to the different security issues in the way settled from a mobile node to the planned fixed node, by observing and controlling the action of the malevolent nodes in the hybrid network shapes the inspiration of the research [4].

2. Related Work

In the literature survey, lots of strategies have been proposed for inter connecting internet with MANET and the techniques used for calculation and management of trust and the security measures considered. Gateway discovery is done by the three approaches namely reactive, proactive and hybrid by extending AODV routing protocol that are addressed by Ali Hamedian et al. [8], very few papers focused on secure data transmission between fixed node in internet and a mobile node in MANET.

P.N.Rajand P.B.Swadas proposed Detection, Prevention and Reactive AODV Scheme (DPRAODV) [9]. Algorithm improves the packet delivery ratio but it generates higher routing overhead and end-to-end delay.

Mistry N, Jinwala DC, IAENG, Zaveri M [10] ImprovedAODV protocol by adding new table and a new timer.Proposed method can achieve high packet delivery ratio but
End-to-end delay is high.

Sanjay K. Dhurandher, Mohammad S. Obaidat, Karan Verma, PushkarGupta, and PravinaDhurandher[11]implemented a strong method to bear the cost of security for MANETs and performs superior to the trust depended mechanisms through it has been analyzed. The friends sharing method ends up being a proficient instrument to open out data of trustworthy nodes adequately in framework. Faultiness of a node is on the solitary circumspection of a specific node that decides from tasks. In their protocol, they have used difficulties besides other secure protocol which uses multi hop routing & records the neighbors work to verify any node contrasted and because of these difficulties, the FACES mechanisms works more preferable & gives much security over the other multi hop routing protocol.

Ayesha, Sridevi and Arshad[12] have proposed an algorithm for moderating black hole attack in AODV protocol based on secure knowledge. It focuses the packets which are sent in promiscuous mode to guarantee that the packets are conveyed to its destiny before concluding that a particular node is black hole node, our algorithm monitors the node for packet drop reason, in this way keeping a trusted node from turning into a black hole node. But to have effectiveness of the data transmission, authentication of the nodes is also required where we can conclude that the data is being transmitted through trusted nodes in a secure route.

Yichi Zhang, Lingfeng Wang and Weiqing Sun[13] focused on the important aspects of the trust system deployment that are static trust node placement, dynamic optimal communication between the selected nodes and a routing algorithm which is fault-tolerant and cost-sensitive. As the nodes in MANETS are dynamic in nature it would not provide the node placement and optimal communication between the mobile node in MANET and the fixed node in internet is achieved through the authentication system based on trust values.

Chen Xi, Sun Liang, Ma Jianfeng and Ma Zhuo[14] have proposed a new scheme for trust management to utilize the certificate chains based on behavior feedback in which the fast-moving nodes realize the mutual identity authentication by, and the identity trust relationship is built up in certificate graph format. On the other hand, to Verified Feedback Packets the successors generate each positive feedback behavior to realize the mutual authentication of forwarding behavior, and consequently the behavior trust relationship is formed.

Pirzada et al. [15] proposed the efficacy of trust-based reactive routing protocols in the presence of attacks. It considers first hand information to evaluate other nodes' trust values. Thus, trust evaluation is restricted to direct neighboring nodes.

In the survey many of the proposed models [9,10,11,12,13,14,15,16, 17, 18, 19, 20, 21] are for providing security and identifying malicious nodes and protecting the data from unauthorized user and these papers are limited to only MANET region but to provide effective communication, mobile nodes have to utilize

the internet resources. So our proposed model increases the application domain of MANET by interconnecting with internet so as to resolve the attack in IIM.

So in this paper, Black Hole attack is studied under the AODV+ routing protocol and its effects are elaborated by stating how this attack disrupt the performance of MANET. Very little attention has been given to the fact to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. There is a need to address both these types of protocols as to analyse black hole attack effect on MANET.

3. Proposed System

In our approach, every node in a network listens to its neighboring nodes promiscuously. In promiscuous mode, every node monitors the packet being forwarded by its neighbors in order to observe the behavior of neighbor regarding packet operation. Every node compares the neighbor information with the information it stores in its knowledge table. If both are same the node assumes that the packet is forwarded further, otherwise node waits for particular amount of time and checks the reasons for packet dropping. In order to confirm packets are sent to its neighbor, the nodes monitor the control packets as well as data packets to prevent selective dropping, as black hole attack drops selected packets. In order to monitor the forwarded packets, every node has to maintain knowledge tables with following entries: fm, rm if the values differ, the nodes are black hole nodes. If node does not forward the packet than the node at the instance checks the other reason for packet dropping, specified in our algorithm. If the packet dropping reaches to a threshold value the node is identified as malicious node and is removed from route selection. It first checks, whether the next node is destination node or not, and also checks the TTL, if its same then it checks node properties such as residual energy(ce).

Knowledge table contains the information about the packet which is most recently transmitted. When any node detects a black hole node in a network, it broadcasts the node's id to other nodes so as that the malicious node can be avoided in routing process. Our algorithm is based on AODV+, where the best path is based on minimum hop and maximum sequence number.

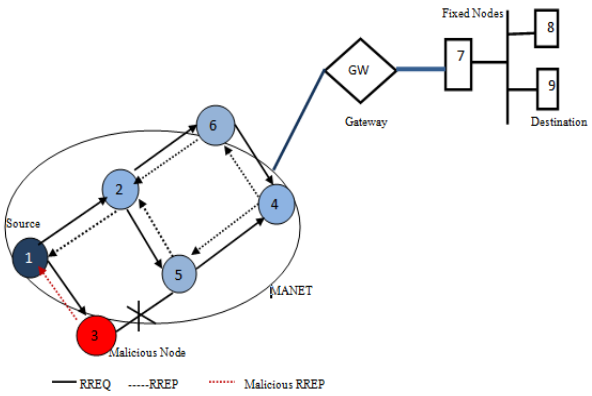

Fig. 2 Black Hole node in IIM

When source wants to send the information to destination, it broadcast the control packet RREQ to its entire neighboring node. RREP is generated by destination through trusted nodes only, if any node is found malicious during route discovery process, its information is transmitted to all other nodes. If already a route is established and later it learns that one of the nodes of its route is a black hole node than the source node removes that node and re-initiates the routing process.

The existing AODV is modified by considering other parameters that also cause packet loss in order to minimize the risk of having a black hole node in the route from source to destination, thereby increasing the throughput and reducing the packet loss.

1. Source node starts sending the RREQ packet in order to establish the route to the destination node.
2. Intermediate node receives RREQ, if it has a route to destination the intermediate node sends RREP to the source node else it broadcasts it to its neighboring nodes.
3. Intermediate node enters into promiscuous mode maintaining secure knowledge table.
4. Secure Knowledge Table maintains two fields 'fm' and 'rm',

'fm' maintains recent packet forwarded,

'rm' maintains the information of neighboring node related to recent packet.

i. If fm= rm, the node is trusted node
ii. If fm is not equal to rm, and energy of the node = threshold, packet drop is due to energy
iii. If fm is not equal to rm, and energy of the node is not equal to threshold,check TimeToLive(TTL) of the packet, if TTL = 0. Packet drop is due to TTL
iv. If fm is not equal to rm, and energy of the node is not equal to threshold, and TTL is not equal to 0, and packet drop = threshold, then node is a black hole node.
5. When a black hole node is deducted in the route from source to destination, RREQ packets are again broadcasted to find a new route to the destination.
6. Then this fresh route is selected and used for transmitting packets from source to destination.

Thereby, this path helps us in improving the throughput by reducing the packet loss due to malicious node.

4. Results

We evaluate the performance of proposed work using the ns-2 simulator with the necessary extension and evaluated the Throughput, Packet Delivery ratio, and end to end delay with respect to number of nodes.

Total Number of Nodes	100
Size of network	600 * 600
Medium access control	802.11
Radio Propagation Range	Two hundred and fifty meter
Time of Simulation	900 sec.
Traffic Source	Constant bit rate
Packet Size	Five hundred and twelve
Model of mobility	Random Way Point mobility
Speed of node	Two, four, six and twelve m/sec.

Table 1.SimulationParameters Used

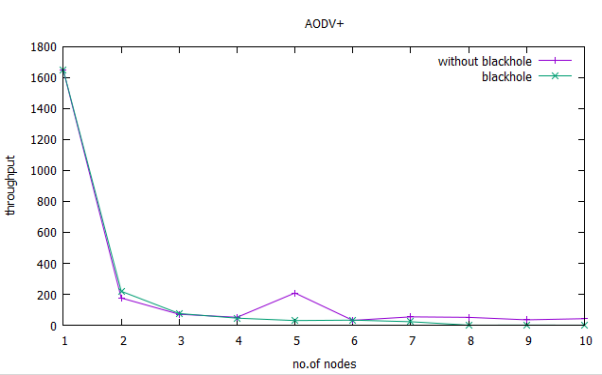

Fig. 3 Comparison of throughput with and without black hole node

Fig. 3 illustrates the throughputs detected by malicious node and without malicious node in AODV+ routing protocol. By comparing the results we observe that throughput is higher at node 1 later decrease at node 2.Again increased at 4 and 5 due to the absence of malicious node whereas at malicious node throughput is lesser in AODV+.

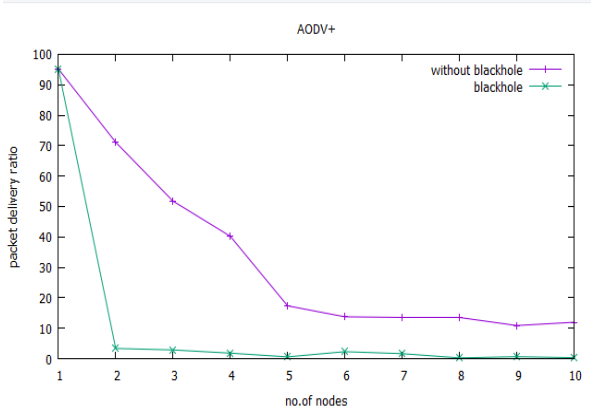

Fig. 4 Comparison of packet delivery ratio with and without black hole node

Fig. 4 shows the comparisons of packet delivery ratio of malicious and trusted nodesin AODV+ routing protocol. By comparing the results we observe that pdr is more at the trusted node through which the data is transmitted in a secure manner to the destination. Whereas at the malicious node pdr is less in AODV+ because the data packets are dropped .

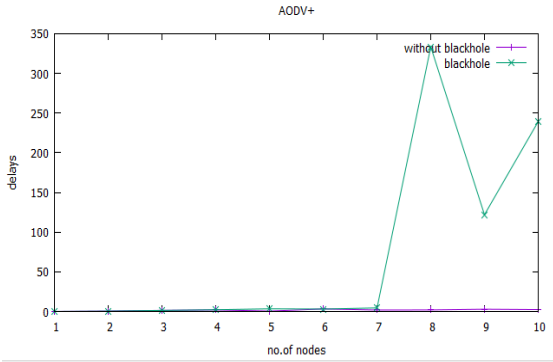

Fig. 5 Comparison of delay with and without black hole node

Fig. 5 describes the delay detected by malicious and trusted nodes in AODV+ routing protocol. By comparing we observe that the data is securely transmitted at the destination side with less or no delay by trusted node whereas at the malicious node delay is higher in AODV+.

5. Conclusion

After performing analysis to identify which routing protocol is more vulnerable to Black hole attack, it is identified that performance of AODV+ is more affected than proposed technique. Therefore this technique can perform under black hole attack without much interruption. But AODV+ cannot perform well under the attack.Therefore a security solution for AODV+ routing protocol mustbe implemented to mitigate black hole attack.

Our future work, we will extend the proposed scheme by implementing using the concept of secret keys for encrypting the data to improve the security of data transmission in IIM.

References

[1]. Kumar, R., Misra, M. and Sarje, A.K., 2007, December. An efficient gateway discovery in ad hoc networks for internet connectivity. In *Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on* (Vol. 4, pp. 275-282). IEEE.

[2]. Jisha, G., Samuel, P. and Paul, V., 2016. Role of Gateways in MANET Integration Scenarios. *Indian Journal of Science and Technology*, *9*(3).

[3]. Wakikawa, R., 2002. Global connectivity for IPv6 mobile ad hoc networks. *Internet-Draft, draft-wakikawa-manet-globalv6-02. txt*.

[4]. Manoharan, R. and Mohanalakshmie, S., 2011, June. A trust based gateway selection scheme for integration of MANET with Internet. In *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on* (pp. 543-548). IEEE.

[5]. Boukerch, A., Xu, L. and El-Khatib, K., 2007. Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, *30*(11), pp.2413-2427.Kagal, L., Finin, T. and Joshi, A., 2001. Trust-based security in pervasive computing environments. *Computer*, *34*(12), pp.154-157.

[6]. Sarvanko, H., Höyhtyä, M., Katz, M. and Fitzek, F., 2010, May. Distributed resources in wireless networks: Discovery and cooperative uses. In *Fourth ERCIM Workshop on Emobility* (p. 51).

[7]. Raj, P.N. and Swadas, P.B., 2009. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. *arXiv preprint arXiv:0909.2371*.

[8]. Dhurandher, S.K., Obaidat, M.S., Verma, K., Gupta, P. and Dhurandher, P., 2011. Faces: Friend-based ad hoc routing using challenges to establish security in manets systems. *IEEE Systems Journal*, *5*(2), pp.176-188.

[9]. Siddiqua, A., Sridevi, K. and Mohammed, A.A.K., 2015, January. Preventing black hole attacks in MANETs using secure knowledge algorithm. In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on* (pp. 421-425). IEEE.

[10]. Zhang, Y., Wang, L. and Sun, W., 2013. Trust system design optimization in smart grid network infrastructure. *IEEE Transactions on Smart Grid*, *4*(1), pp.184-195.

[11]. Soltanali, S., Pirahesh, S., Niksefat, S. and Sabaei, M., 2007, June. An efficient scheme to motivate cooperation in mobile ad hoc networks. In *Networking and Services, 2007. ICNS. Third International Conference on* (pp. 98-98). IEEE.

[12]. Pirzada, A.A. and McDonald, C., 2004, January. Establishing trust in pure ad-hoc networks. In *Proceedings of the 27th Australasian conference on Computer science-Volume 26* (pp. 47-54). Australian Computer Society, Inc.

[13]. Mohammad, A.A.K., Mirza, A. and Razzak, M.A., 2015. Reactive Energy Aware Routing Selection Based on Knapsack Algorithm (RER-SK). In *Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2* (pp. 289-298). Springer International Publishing..

[14]. Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks. *Indian Journal of Science and Technology*, *9*(26).

[15]. Siddiqua, A., Sridevi, K. and Mohammed, A.A.K., 2015, January. Preventing black hole attacks in MANETs using secure knowledge algorithm. In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on* (pp. 421-425). IEEE.

[16]. Sana, A.B., Iqbal, F. and Mohammad, A.A.K., 2015, January. Quality of service routing for multipath manets. In *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference on* (pp. 426-431). IEEE.

[17]. Mohammad, A.A.K. and Atheeq, C., MUTUAL AUTHENTICATED KEY AGREEMENT SCHEME FOR INTEGRATED INTERNET MANETS.

[18]. Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Energy Aware Routing For Manets Based On Current Processing State Of Nodes. *Journal of Theoretical and Applied Information Technology*, *91*(2), p.340.

[19]. Mohammad, A.A.K., Mirza, A. and Vemuru, S., 2016. Analytical Model for Evaluating the Bottleneck Node in MANETs. *Indian Journal of Science and Technology*, *9*(31).

[20]. Atheeq, C. and Rabbani, M.M.A., 2016. Secure Data Transmission in Integrated Internet MANETs Based on Effective Trusted Knowledge Algorithm. *Indian Journal of Science and Technology*, *8*(1).

[21]. C.Atheeq, M.MunirahamedRabbani "Effective cluster key mechanism for integrated internet MANETs " *International journal of applied engineering research vol.10 No.44, 2015*