Trust-based Multiple RREPs Approach for Black Hole Attack Prevention in MANETs

Arshad Kamaal
Sobhasaria Engineering College
Rajasthan Technical University
Sikar, India

Anwar Husain Joya
Sobhasaria Engineering College
Rajasthan Technical University
Sikar,India

.

***Abstract*— Blackhole attacks (BHA) are one of MANET's most serious security issues. The malicious node destination node is performed from sending fake RREP towards source node that initiates route search & loses data traffic by the source node. Because of design flaws essential to routing protocols (RPs) into MANETs, several researchers have adopted various methods towards suggesting several kinds of defense mechanisms via the black hole problem. BHA is one of the most widespread active attacks that reduce network performance and reliability as a result of dropping packets coming through a malicious node. The purpose of black-hole node (BHN) is to trick every node of NW that wants to communicate with another node into thinking there is always a better route to destination node. AODV NW has a non-reactive RP to detect & deactivate BHNs. In this research, we have improved AODV by incorporating a new lighting technology that relies on trusted multiple RREPs to prevent BHA. The proposed technique is applied with NS-2.35 simulation tool. Results of proposed technique in positions of throughput, Routing above & Packet Delivery Ratio are so close towards original AODV deprived of a black hole.**

***Index Terms*— MANET, Black Hole Attack (BHA), AODV Routing, Black Hole Prevention, Route Reply, Multiple RREPs, Trust-based Multiple RRSPs.**

I. Introduction

MANET is gathering of wireless hosts that may subsist organized quickly to multi-hop packet radio NWs lacking the help of conventional infrastructure or a centralized administrator. MANETs have certain unique aspects, for example, untrusted wireless media (link) utilized to communicate among hosts, constantly changing NW topology & membership, battery, limiting bandwidth, lifespan, & computing power of nodes. MANET is susceptible to several kinds of attacks. This comprises passive monitoring, active engagement, impression, and DOS. One of the most serious issues into MANETs is vulnerability of routing protocols (RPs). One of the most general utilization RPs into MANETs is AODV-RP [1]. This is the source that started On-demand RP. But, AODV is susceptible to known BHA [2].

BHA intends that one or multiple malicious nodes violate routing rules and drop all received packets. Malicious nodes are able to achieve their misbehaviors in many ways. It is often seen black hole attacks in MANETs [3]. An example of a black hole node with a forged route reply (RREP) packet is presented as Figure. 1[4].

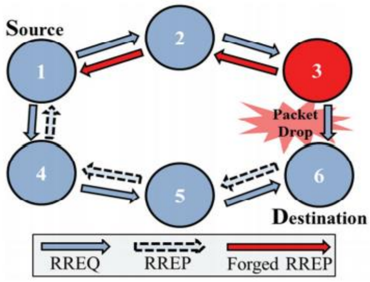

Fig. 1. A black hole attack based on forged route reply packet

The source node is node 1 & node 6 is a destination node. Node 3 is a malicious node that sends forged RREP packets. In an example, a source node sends route requests (RREQ) towards its neighbors as well as node 2 and node 4 for establishing a path towards destination. The node 4 forwards RREQ packet towards node 5 formerly node 5 forwards it to destination node. After that, node 6 replies RREP packet and states that it is destination node. However, on another path, node 2 forwards RREQ packet towards node 3. In general, node 3 should forward RREQ packet to node 6 for establishment of routing path but this is a black hole node (BHN). Malicious node, as well as node 3, send forged RREP packet & rights that it has shortest path towards destination. Moreover, node 3 drops received RREQ packet sent by node 2 and do not forward it to destination. Network operation breaks down under incorrect routing due to malicious node 3. Consequently, network suffers from unsatisfying PDR caused by attack from BHN.

The overall paper has organized as following. Next, we have delivered a summarized overview towards BHA using Multiple RREPs in MANET into Section II & define related work of BHA into Section III. In Section IV, we deliver a complete explanation of the proposed technique. We consider the performance of the proposed technique & relate it by remaining protocol by complete simulation into Section V. Lastly, Section VI determines paper.

II. Blackhole Attacks using Multiple RREPs in MANET

The malicious node performs as a black hole, causing every data packets passing by it to go from energy and matter such as our universe in this attack. Uncertainty an invasive node is connecting node of 2 connecting elements of NW, this efficiently divides NW into 2 disconnected modules. Now black-hole node divides NW into 2 parts [5].

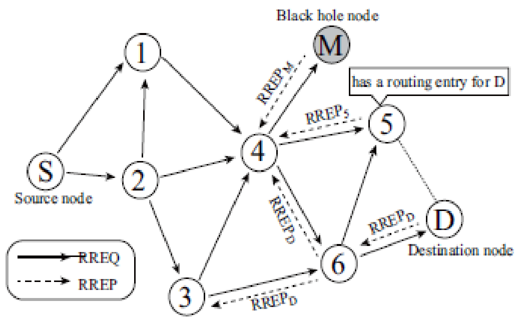

Fig. 2. An example of multiple RREPs forwarding

An example of several RREPs is shown in Fig. 2. In this specimen, source node S shows an RREQ to the destination node. Intermediate nodes 1–4 & 6 send RREQ back to their neighbors. Node 5 in this example already has routing entry via D, & that path is 5-D. Node 5 responded towards RREQ by integrating RREP5 into S. If RREQ reaches D via S→2→3→6→D path, formerly D respond towards RREQ with integrating RREQ onto S. After receiving RREPD from D, node 6 produces 2 copies of RREPD & delivers to node 3 & 4, correspondingly. Node 6 has 2 routing entries by several next-hops, namely Node 3 & Node 4 into its routing table S got 2 RREQs by Node 3 & Node 4 correspondingly. BHN M sends it to the RREPM node in this example. RREPM is simulated RREP by small hop count & spoof destination location number. One of the received RREPs detects an incorrect RREP node 4, namely, RREP5, RREPD, and RREPM, preventing a BHA using an RREP filtering mechanism in particular.

Some strategies to moderate issue:

i Collect more than one RREP message (more than two nodes) so that multiple routes to the destination route do not get redundant and buffer packet protected routes.

ii A table is maintained at every node by prior sequence no. in incremental order. Every node increases sequence no. before the packet is exchanged. The sender node passes RREQ to a neighbor, & when it arrives at RREQ destination, the last packet answers with serial number with RREP. Uncertainty intermediate node detects that RREP has an invalid sequence no., it detects that something went wrong.

III. Literature Survey

Taku Noguchi and Mayuko Hayakawa [2018] to prevent BHA, it proposes a new threshold-based BHA defense method with several RREPs. Towards examine the performance of the proposed technique, we related it to current approaches. Our simulation outcomes demonstrate that the proposed technique outperforms current approaches by standpoint of throughput, packet delivery rate & routing overhead. [6].

Hammamouche et al. [2018] Suggest solutions based on nodes' reputation & multi-hop recognition. The popularity of nodes increases or decreases depending on position & position of observation. When a node's reputation is below the threshold, it will be studied BHN. PM is simple & cooperative to detect & evade black hole attackers & facilitate collaboration between NW nodes. By simulation, we associate PM with simultaneous protocol, & we display search ratio & its proficiency in communication overhead [7].

Taku Noguchi and Takaya Yamamoto [2017] suggest a novel threshold-based BHA anticipation technique. To examine the performance of the proposed technique, we related it by remaining approaches. Our simulation outcomes demonstrate that the suggested technique outperforms remaining approaches by standpoints of BHN detection rate, throughput, and packet delivery rate [8].

P. S. Hiremath et al. [2016] An innovative technique to detect & prevent BHA on MANETs has been developed. The proposed technique is founded on an adaptive fuzzy transition system (AFTS) via MANET to identify and avoid supportive BHA. The popular protocol used in MANET is the AODV protocol, which is replicated with NS2. Simulated outcomes of the suggested technique are related by the adaptive process [17] in which source node confirms performance of every node through DAT table that declares BHN with channel overhearing that is node-to- Contains node-to-next-node information technique. It is perceived that suggested technique founded on the adaptive fuzzy logic system outperforms adaptive technique in provisions of the Throughput, End-to-End Delay & PDR. [9].

Arathy K Sa and Sminesh C N [2016] Suggest a new strategy to detect single & cooperative BHA with minimal routing & computational overhead. Identifying single & several BHNs with an additional route request by a specified address that does not have specified D-MBH algo calculates boundary ADSN, constructs blackhole list, & suggested D-CBH Algo requests. D-CBH algo generates a list of cooperative BHNs by ADSN, black hole tables & next hop data removed by RREP [10].

A. Gupta [2015] Suggest a novel technique RTMAODV (Real-Time Monitoring AODV). It doesn't present some overhead. Additionally, black holes can be detected & blocked by a neighbor's node with real-time monitoring. Novel suggested technique is effective via several instructional sessions. The broadcast concept is utilized in this way. Node reacting to root request (RREQ) with a source is examined into Prometheus mode. Malicious node detection is a truly neighbor node of the sender node of root replication (RREP). In a simulation, the new method shows better results in terms of PDRs than AODV RP in the occurrence of a malicious node in BHA. [11].

N. Choudhary and L. Tharani [2015] A new solution against BHA is suggested. It paper shows a timer-based detection method via BHN detection. We suggested a timer-based technique into the network layer towards listening to \ next node action. Imitation outcomes with EXata-Cyber suggest that very malicious nodes may be identified in dynamic NW & result in improved PDRs. [12].

Ming-Yang Su [2011] various IDS (Infiltration Detection System) nodes have been organized on MANET to detect & prevent selective BHA. IDS nodes should be set in a sniffing method towards executing ABM (anti-blackhole mechanism) function, which is mostly utilized towards evaluate node's suspect value node. While threshold value is exceeded, a pass IDS transmits a block message, informs all nodes in NW, & signals malicious node to cooperate. This study uses NS2 towards authenticating effect of suggested IDS organization, because IDS nodes may quickly stop malicious node deprived of false-positive uncertainty specified threshold is set. [13].

IV. Proposed Methodology

The proposed technique studies the generator node of RREP to have advanced average RREP sequence no. then a threshold value, & trust value is below threshold value as BHN. The specific technique permits several RREPs to be sent via the same RREQ packet, allowing every node towards finding a very reliable average serial no. data. The proposed technique is towards improving acceptable routing overhead with packet delivery rate and throughput.

Proposed algorithm:

1. Initialize the network
2. Describe source node S & destination node D
3. Path establishment process in AODV
   - i The source node shows RREQ towards its neighbors.
   - ii Node getting RREQ tests even if there has entry via D node into their routing table.
   - iii This broadcasts again RREQ as long as there is a no entry or old entry via D into their routing table.
   - iv Uncertainty node that established RREQ be an intermediate node or a D node which have new adequate entries via destination into its routing table, intermediate / destination node replies through unicasting RREP packet back towards S node.
   - v RREP packets are moved back towards S node beside turn around way namely set up while RREQ is forwarded.
   - vi The bidirectional way among S & D nodes is conventional from stages i–v.
4. Update / Create average sequence table entry
5. Computes threshold *TH*dstIDcurrent dynamically created on its average sequence no. table.
6. Compute the trust value of every RREP as a ratio among no. of packets dropped & no. of packets forwarded.
7. checkered if created/updated *avgSQ* of corresponding entry is greater than *TH*dstIDcurrent & similarly check trust
   - i Every node detects events of its neighbor node & reports towards 'knowledge' cache.
   - ii before the generator node (*genID*current) of RREP is observed like black hole node
   - iii RREP produced through the node of the *genID*current is discarded.
8. Uncertainty hop counts of RREP is 1, node tests even if *genID*current is similar to IP address of the node by that RREP has expected (this is found by source IP address into IP header).
   - i The uncertainty is not similar, RREP is rejected.
   - ii Uncertainty RREQs are not rejected, the rest of the procedure is fully similar by original AODV operation.
9. Exit

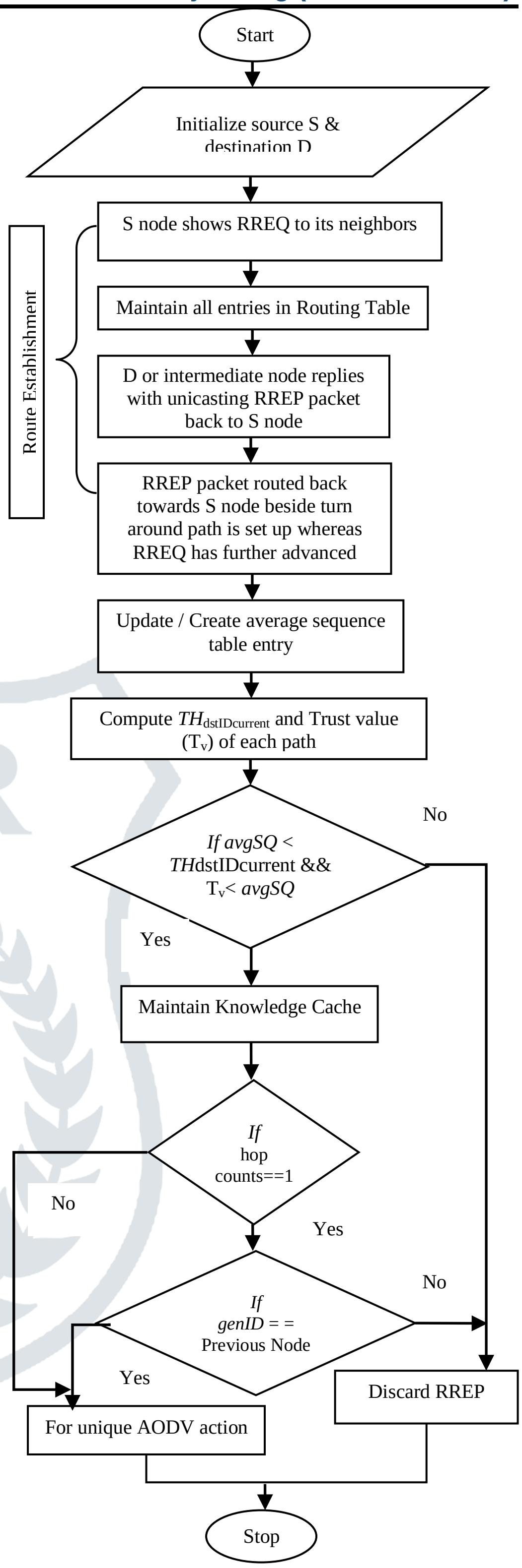

Fig. 3. Proposed flow chart

V. Result Analysis

In this section, we describe our investigation of the performance of the proposed method (PM) in comparison to existing methods. For our simulation, we applied network simulator NS-2.

Table I: Simulation Parameters

Parameter	Value
Simulation time	100 [s]
Number of nodes	20, 25, 30, 35
Network area	1186 * 584 [m]
Mobility model	Random Waypoint
Transport layer protocol	UDP
Application type	CBR
Data packet size	512 [bytes]
No. of BH nodes	0, 1, 2, 3
Parameter *MAX*rrep	3

1) Normalized routing overhead: Normalized routing overhead is defined by the following equation:

$$Normalized\ routing\ overhead = (Nctrl/Nrecv) * 100$$

Here, *N*ctrl is total no. of all control packets transfer in all nodes.

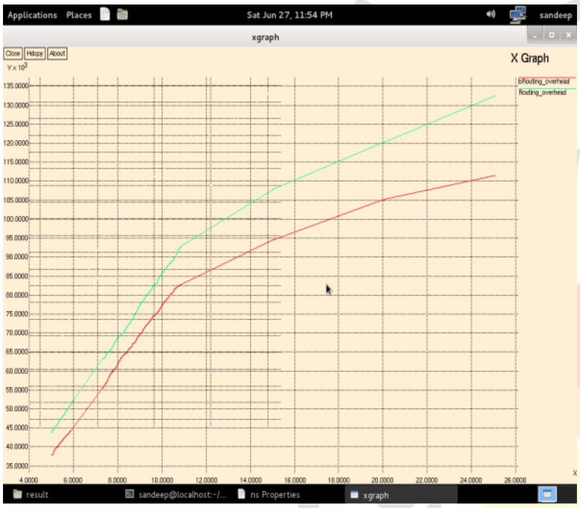

Fig. 4. Routing overhead

Figure 4 displays normalized routing overhead characteristics for the PM and the existing method. As shown in this figure, PM achieves maximum routing overhead in comparison to an existing protocol.

2) Packet delivery rate PDR:

$$PDR = (N_{rec}/N_{sent}) * 100$$

Here, *N*recv is total No. of data packets usual in destination node, & *N*sent is total no. of data packets transfer in source node.

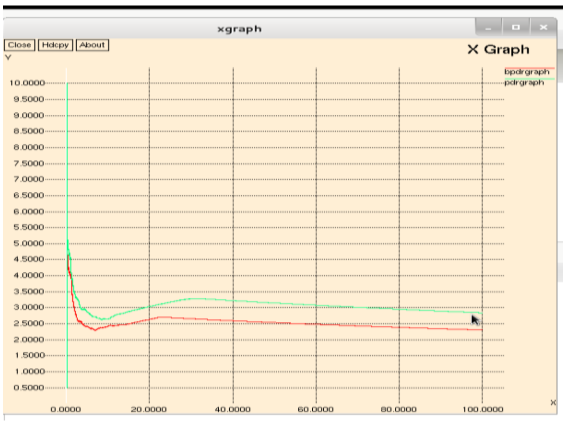

Fig. 5. PDR ratio

Figure 5 shows the packet delivery rate performance of PM & current method. As shown in this figure, PM achieves a higher packet delivery rate than the current method. In PM, trust-based multiple RREP filtering systems with dynamic threshold contributes to optimally dropping simulated RREP. As no .of nodes increases, the packet delivery rate of the proposed method decreases. No. of nodes receiving false RREP causes an increase in no. of nodes. In this case, PM mistakenly leaves valid RREP due to actual average sequence no.

3) Throughput: Throughput is distinct from the following calculation.

$$Throughput = (PktSize * 8 * Nrecv)/T$$

Here, *PktSize* is data packet size, & *T* is the time elapsed as of time source node receives 1ST RREP to termination of simulation.

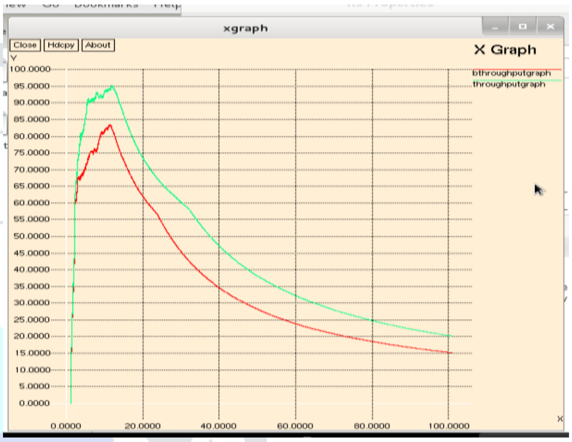

Fig. 6. Throughput

Figure 6 shows the throughput presentation for PM & existing methods. PM achieves better quantity enactment than & existing method by BHA.

VI. Conclusion

In recent times the security issues include a great challenge in the routing protocols in MANETs. In MANETs, the most known security threats are BHA. We have proposed a new threshold-based BHA defense method that usages multiple RREP forwarding & RREP filtering systems based on dynamically updated average serial no. information to protect against blackhole attacks in AREVs. Experiments have found the effectiveness of PM using various performance matrixes. Simulation results show that PM recovers packet transfer enactment, quantity but regulated routine above is still high. There is no doubt at all that the collaborative black hole detection method will still be a hot research issue in the future. In our opinion, a hybrid routing protocol is essential to improve defects of reactive & proactive routing protocols.

References

[1] Perkins, E. Belding-Royer, and S. Das, "Ad-hoc on-demand distance vector (AODV) routing", Internet-Draft, RFC 3561, July 2003.

[2] Sonia and Abhishek Aggarwal, "A Review Paper on Pooled Black Hole Attack in MANET", International Journal of Advanced Research in Computer Science and Software Engineering 3(5), May - 2013, pp. 372-375.

[3] F. H. Tseng, L. D. Chou, and H. C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks," Human-centric Computing and Information Sciences, vol. 1, article no. 4, 2011.

[4] Fan-Hsun Tseng, Hua-Pei Chiang, and Han-Chieh Chao, "Black Hole along with Other Attacks in MANETs: A Survey", J Inf Process Syst, Vol.14, No.1, pp.56~78, February 2018.

[5] Aniruddha Bhattacharyya, Arnab Banerjee, and Dipayan Bose, "Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques", arxiv, 2011, pp. 1-11.

[6] Noguchi, T., & Hayakawa, M. (2018). Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 539-544.

[7] Hammamouche, A., Omar, M., Djebari, N., & Tari, A. (2018). Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. Journal of Information Security and Applications, 43, 12–20.

[8] Noguchi, T., & Yamamoto, T. (2017). Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks. Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, pp. 797-802.

[9] P. S. Hiremath, Anuradha T and P. Pattan, "Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs," *2016 International Conference on Information Science (ICIS)*, Kochi, 2016, pp. 245-251.

[10] Arathy, K. S., & Sminesh, C. N. (2016). A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET. Procedia Technology, 25, 264–271.

[11] A. Gupta, "Mitigation algorithm against black hole attack using Real-Time Monitoring for AODV routing protocol in MANET," *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2015, pp. 134-138.

[12] N. Choudhary and L. Tharani, "Preventing Black Hole Attack in AODV using timer-based detection mechanism," *2015 International Conference on Signal Processing and Communication Engineering Systems*, Guntur, 2015, pp. 1-4.

[13] Su, M.-Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications, 34(1), 107–117.