JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 08, 2020

SECURE ROUTING FOR PREVENTION OF BLACK HOLE ATTACK USING RELIABILITY VALUE BASED ALGORITHM

Ruby D*[1], Gayathri A[2], Gopalakrishnan T[3], Santhosh SVN[4], Selvi M[5], Kannan A[6]

[1, 3, 5] Assistant Professor (Sr.G), School of Computer Science and Engineering, Vellore Institute of Technology, Vellore

[2, 4] Assistant Professor (Sr.G), School of Information Technology and Engineering, Vellore Institute of Technology, Vellore

[6] Senior Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Vellore

[1]ruby.d@vit.ac.in, [2]gayathri.a@vit.ac.in, [3]gopalakrishnan.t@vit.ac.in, [4]santhoshkumar.svn@vit.ac.in, [5]selvi.m@vit.ac.in, [6]kannan.a@vit.ac.in

Abstract

Mobile Ad-hoc NETworks (MANETs) are the self-configuring network consisting of mobile nodes communicating via radio waves. These networks do not have any centralized controlling mechanism and designated routers. All the nodes in the network can be either a communication end point or a router. Therefore, MANETs are more vulnerable to attacks. Black hole attack is a popular attack in MANETs routing protocols particularly in Ad hoc On-Demand Distance Vector (AODV). In this paper, we propose a novel algorithm to detect and prevent the black hole attacks. For this, we calculate Reliability Value (RV) of all nodes to identify malicious nodes. In this paper, RV is used to find the best path among k number of paths to keep away from the malicious node. The experimental results show that the black hole attack has been detected and prevented and the performance of the network has been increased.

Keywords: MANETs, AODV, Vulnerable, black hole attacks and Reliability Value.

I. INTRODUCTION

Due to increasing popularity of wireless devices, wireless networks are becoming an inevitable technology. Basically, wireless networks, which connect wireless nodes with the help of radio waves, are categorized into two types. One is Infrastructure-oriented and the other is Infrastructure-less. In Infrastructure-oriented networks, the networks need Infra structure to operate on. The Infrastructure is a centre part through which all the mobile nodes are connected. This centre part is called as access point and it is connected with internet through wired medium. All the network traffics are routed through this access point.

The second type of network is called as Infrastructure-less or MANETs. In this type of networks, there is no infrastructure present and the communication is done through the nodes itself. The nodes act both as communication end points (sender and receiver) and routers and the mode of transfer is through radio waves. The general

MANETs is explained by Sadia et al. [2018]. Figure 1 shows the overview of MANETs by Ochola *et al.* [2017]. The mobility nature of the nodes in the MANETs makes it very difficult to manage, because the topology of the network is more dynamic. It also adds complexity to manage the routing table of mobile nodes.

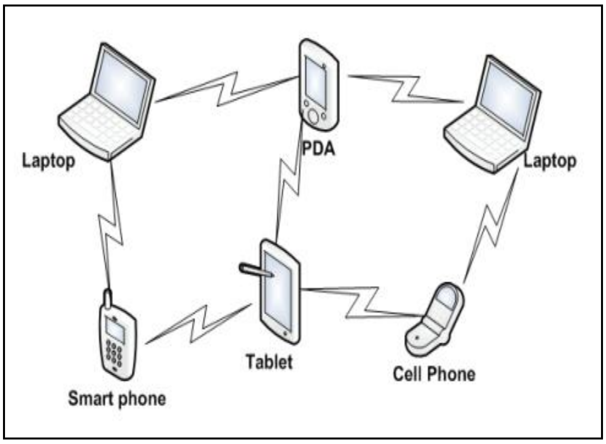

Figure 1: MANET – overview.

The routing process in MANETs is done through various algorithms as described in Geethu *et al.* [2013] are categorized in to 3 types. They are proactive, reactive and hybrid.

In this, the proactive protocol works in the concept of table driven. All the mobile nodes maintain routes to all other nodes in a table. This algorithm is not suitable for large networks as the table entries are very large. Some of the examples of this type are Destination Sequenced Distance Vector Routing (**DSDV**) and Fisheye State Routing (**FSR**).

The second type of protocol is Reactive, which is explained in Patel *et al.* [2014]. In this protocol, the routes are created on demand. When a sender wants to send a packet, it establishes a route to the destination by broadcasting Route-REQuest (RREQ) message. The intermediate nodes, on receiving this, will forward the RREQ to other nodes (either intermediate or receiver) after updating the back link in the message. When the receiver receives this, it replies backwards with the Route-RESponse (RRES) message to the sender through the intermediate nodes. Thus the route is established for communication. Some of the algorithms in this category are Dynamic Source Routing protocol (**DSR**) and **AODV**.

The last type of protocol is Hybrid. Zone Routing Protocol (ZRP) which is one of the best example for this type. This type of protocol is used specifically in a very large network. The network is divided into number of subnets called Zones. The intra zone nodes use reactive routing and the inter zone routing is done with proactive protocols.

The MANETs are more vulnerable to security breaches, because of its open medium and lack of centralized control mechanisms. The common attacks explained in Srinivas *et al.* [2016] are flooding attacks, black hole attacks, impersonation attacks and node location reveal attacks.

In the above listed attacks, AODV is mainly vulnerable to black hole attacks Xiaobing *et al.* [2000]. These attacks are generated from one or more compromised nodes in the MANETs. The malicious nodes (M), like other nodes, get the RREQ message and reply immediately back to the sender(S) as if they have the route to the destination node without any further delay. Thereby, the sender thinks that this route is the fastest route and starts its communication through this node. This is depicted in Figure 2. All the packets will be dropped by this node deliberately as it doesn’t have routes. The other scenario is in which the malicious node acts like normal node at route establishment step. While data transfer, it will drop either all packets or specific packet. These types of attacks are very difficult to discover.

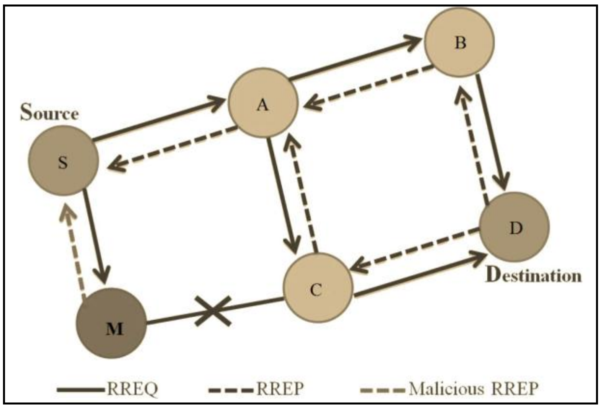

Figure 2: Malicious node in a MANET

The objective of this paper is to provide a novel method to discover a black hole attack in AODV protocol and ignore the malicious node in the further communication. The reminder of this paper is organized as follows. Section II provides a detailed literature work done on black hole attacks and prevention methods. A novel method is proposed to avoid (secure) black hole attack in section III. The results are discussed in section IV and section V concludes and provides the future scope for further research.

II. LITERATURE SURVEY

Muneer *et al.* [2018]introduced various security issues and challenges caused by black hole attacks. Various solutions to detect these attacks like Enhanced AODV protocol by Bani-Yassin *et al.* [2014] and Timer based detection methods by Choudary and Tharani [2015] were proposed.

Ochola *et al.* [2017] discussed the effect of mobility in MANETs to analyze the black hole attack. Various metrics like packet delivery ratio, end-to-end delay and throughput are measured using simulations. If the malicious node is closer to the source, then the performance of the network is degraded.

One of the Light-weight techniques was proposed by Adman and Mahmoud [2018]. In this, they used bait request and timers to identify a black hole node. The bait request is created with a fake destination id and Time To Live (TTL) value is set to 1 to prevent the congestion of fake request message in the network. This request is broadcasted to the network. As the black hole node is having the nature of responding quickly without having connection to destination, it will respond to the source immediately. Thus the black hole node is identified and prevented in the data transfer.

Jaisankar et al. [2010] proposed a method to identify the black hole node. They used the ratio of number of packets dropped to the number of packets forwarded. Once it is identified, the node will be avoided.

Redundant paths were used by Nidhi and Alok [2012] to evade the malicious nodes. It will consider not only first RRES message, the subsequent RRES (at least 3) were also considered to find the authentic paths. They also used sequence number based solution to the problem.

Sink nodes were used by Vikash kumar [2018]. These nodes are placed in the MANETs. The network is divided in to sub networks called grids. One sink node will be identified in each grid. This node will work in promiscuous mode. All the data transfer should be routed through these sink nodes.

Muhammed et al. [2015] used DPS nodes to monitor the network. These nodes will not participate in actual communication; instead it will only keep an eye on all other nodes and record the number of RREQs sent by those nodes. This process work in the fact, that the black hole nodes will not create any RREQ messages.

Sandeep *et al.* [2017] proposed SAODV protocol to detect the black hole and grey hole attacks. They used opinion value received from the neighbour nodes to decide whether to use a particular node for data transfer or not.

Divya and Venkataram [2018] presented a method to identify the attack based on honey pots. The honey pot make use of black hole attack tree to identify the black hole attack in the network and attack history database to confirm the attacks.

Gayathri and Narayanasamy [2015] proposed a new secured S-EAACK methodology to solve the black hole attack using AODV routing protocol. This S-EAACK technique enhances the network performance metrics such as energy, delay and PDR.

III PROPOSED SYSTEM

The objective of the proposed system is to detect a malicious node that causes a black hole attack in AODV routing protocol and prevent it. To achieve this, a Reliability Value (RV) and malicious value are added for each node to the normal routing table entry. A node will calculate and update a Reliability Value of other nodes in its reliability table. This RV can be used to detect both single black hole and cooperative black hole attacks that exist in route discovery steps and in the data transfer steps.

In this proposed, Reliability Value Based (RVB) algorithm, initially all node's RV is set to 1, which is the maximum value. If a node wants to send data, first it has to discover a route to the destination. For this, the source will broadcast a RREQ message to all its neighbouring nodes. These nodes are intermediate nodes (IN) through which the messages are forwarded (routed) to the destination. The IN will in turn forward this message either to nearby IN or destination node.

Each node will update RV in the reliability table in the following condition. a) If the number of RREQ >0 then reset RV=1. b) For every RREQ_TIMER value, all nodes record the number of RREQ messages and drop rates of each other nodes. If there is no RREQ from a node or drop rate falls below the threshold value (α) then the RV value of that particular node is decremented by 0.2. The α value is set, based on traffic load of the network and node intensity.

Now the malicious node is identified by the RV value of that node. If a RV value is lesser than 0.5, then this node is marked as a malicious node and the source node will not use this node for further communication. If a node sends RREQ message, then this node will be marked as non-malicious node by its neighbouring nodes and its RV value is reset to 1. Whenever the source node receives RRES messages from its neighbours, it needs to wait for at least 3 messages from 3 different routes and the routes with malicious nodes has to be excluded. Thus, RVB algorithm avoids the single black hole node attack or cooperative black hole attack based on RV value. The source has to select the best route that has the highest RV value for the communication. If the node has highest RV value, then its drop ratio is very less. So the communication link is more reliable.

Table 1 summarizes the Reliability Value and its description

Table 1: RV value and its Description

WHEN	RV VALUE	OPERATIO N	DESC RIPTI ON
On creation of routing table entry	1	Initialize	Initially, all nodes in the networ k are reliable. Maxim um

			value of RV=1
Minimum one RREQ received from that node	1	Re Initialize	Concluded that the node is not malicious and its RV is reset to maximum value.
Drop rate of a node is greater than average drop rate probability	Decremented By 0.2	Decrement	RV value of the node is decremented, whose drop rate is more
No RREQ till the prescribed RREQ_TIMER	Decremented By 0.2	Decrement	If no RREQ up to certain time, then its reliability value is decremented.
Value of RV is Lesser than 0.5	Lesser than 0.5	Set malicious = yes for that node	If the RV value is lesser than 0.5, then it is not reliable node. So that node is set as malicious node.

Pseudo code for proposed method

```
Assumption: All malicious nodes are one hop distance from the source.
Initialize: RV of all nodes = 1, drop rate of all nodes = 0 and all nodes as non-malicious node.
RREQ_TIMER=10 sec
Calculate drop rate of a node = No. of packets forwarded / No of packets sent.
For every RREQ_TIMER, check number of RREQs.
if number of RREQ received from a node >0  then
Set RV of that node = 1.
end if.
if number of RREQ received from the node is zero or drop rate of a node  > α  then
 Decrease its RV by 0.2
end if.
End for.
if RV of a node < 0.5 then
Set that node as a malicious node.
end if.
Receive RREP from at least 3 nodes excluding the route through malicious nodes.
Use the route which has the neighbouring node with high RV.
```

```
End if.
```

IV RESULTS AND DISCUSSIONS

The simulation of the RVB algorithm is done in NS2 tool and the performance of the proposed algorithm is compared with various existing methods through various parameters such as throughput, packet delivery ratio and end to end delay. The throughput is defined as number of packets delivered (in kbps) in unit amount of time. The ratio to the number of packets received by the destination to the number of packets sent by the source is termed as packet delivery ratio. The end to end delay is described as the time needed by a packet to reach a destination.

Table 2 list out the entire simulation parameters.

Table 2 : Simulation Parameters.

Parameter Name	**Value**
Number of Nodes	Varying from 25 to 150
Protocols used	AODV, RVB with AODV
MAC protocol	802.11
Number of black hole nodes	2
Channel capacity	2.5 Mbps
Radio range of a node	200 m
Packet size	512 bytes
Simulation area	1000 X 1000 m^2
Simulation time	100 s
Node position	Random

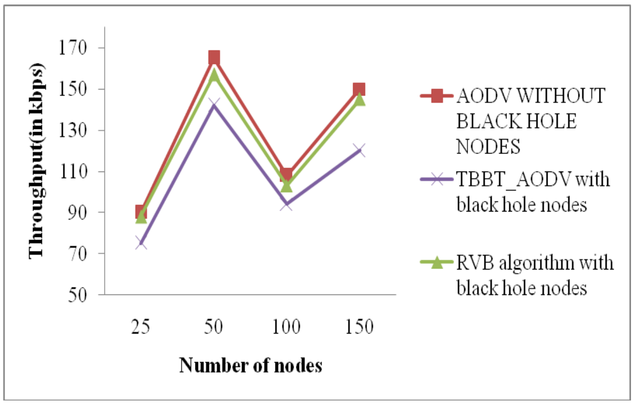

Figure 3: Number of nodes vs throughput

The experiment is conducted with different number of nodes and the throughputs of various algorithms are recorded. From the Figure 3, RVB algorithm exhibits on an average of 14% higher throughput value than the existing TBBT_AODV that was given in Adwan and Mahmoud [2018]. We found that, the throughput of RVB algorithm is nearer to the Native AODV without black hole attack.

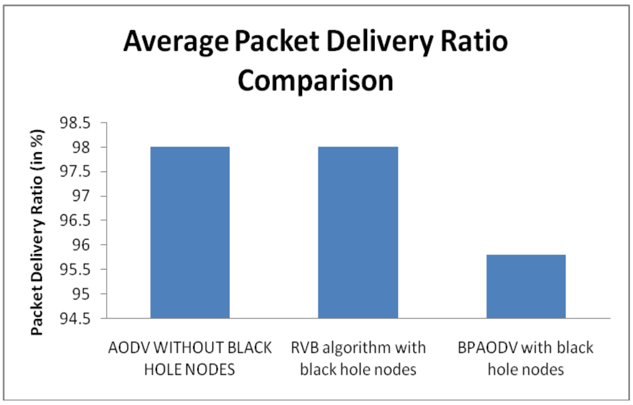

Figure 4: Comparison of average packet delivery ratio

The packet delivery ratios of various algorithms are given in Figure 4. As RVB method consider the path with no malicious nodes, all the packets will be delivered to the destination. We also considered the paths having nodes with better reliability value, which means that we use the nodes with minimum dropping rate. So, the PDR of RVB algorithm is same as of the network with no malicious nodes. From the figure, it is shown that, RVB algorithm out performs the existing algorithm by 2.2%.

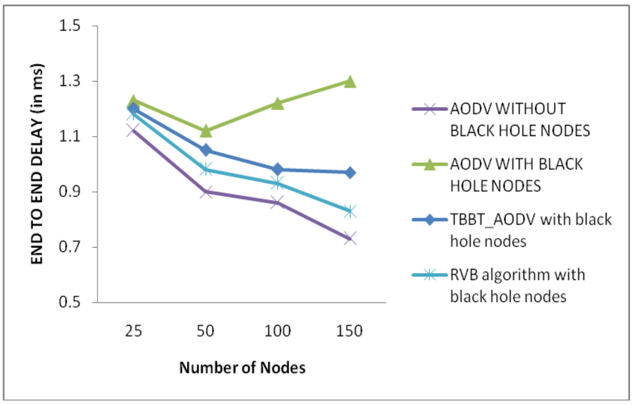

Figure 5: Number of nodes vs End to End Delay

Figure 5 shows the end to end delay comparison of RVB method with the existing method. It is shown that the proposed algorithm exhibited lesser delay value than the existing algorithm, because we use the path with higher RV nodes and the dropping rate of these nodes is very low. From the parameters discussed above, we have shown the effectiveness of the algorithm.

V CONCLUSION AND FUTURE SCOPE

The black hole attacks are the major attacks in AODV protocol. To detect and prevent this attack, we proposed a novel Reliability Value based method. The RV is decremented for the nodes with higher dropping rate and the nodes which have not sent any RREQ messages up to a prescribed time. The simulation results show that the performance of the proposed RVB algorithm is better than the existing algorithms. The simulation is done with random mobility model. In future, other mobility models and other parameters will be considered to further improve the performance of the overall system.

REFERENCES

1. Sadiya Mirza, Sana Zeba Bakshi, “Introduction To Manet”, International Research Journal of Engineering and Technology (IRJET), Vol. 05, Issue 1, 2018.
2. Mohandas G, S. Silas and S. Sam, "Survey on routing protocols on mobile adhoc networks," 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), Kottayam, 2013, pp. 514-517.
3. Patel, Daxeshbhai & Patel, Sejal & Jethwa, Pinakin & Kothadiya, Hemangi & Jhaveri, Rutvij, "A survey of reactive routing protocols in MANET", 2014 International Conference on Information Communication and Embedded Systems, ICICES, 2014.
4. Dilli, Ravilla "Hybrid Routing Protocols for Ad hoc Wireless Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing. Vol .2, pp.79-96, 2011.
5. Aluvala, S, Sekhar, K.R., Vodnala, D, "An empirical study of routing attacks in mobile ad-hoc networks", Procedia Comput. Sci. Vol. **92**, pp. 554–561, 2016
6. Bani Yassein, Muneer & Hmeidi, Ismail & Khamayseh, Yaser & Al-Rousan, Mohammad & Arrabi, Danah, "BLACK HOLE ATTACK SECURITY ISSUES, CHALLENGES & SOLUTION IN MANET", International Conference on Computer Science, Engineering and Information Technology, 2018.
7. Xiaobing Zhang, S. F. Wu, Zhi Fu and Tsung-Li Wu, "Malicious packet dropping: how it might impact the TCP performance and how we can detect it," Proceedings 2000 International Conference on Network Protocols, Osaka, Japan, pp. 263-272, 2000.
8. BaniYassein, M., Khamayseh, Y., & Nawafleh, B. (2014). Improved AODV Protocol to Detect and Avoid Black Hole Nodes in MANETs. FUTURE COMPUTING, 7-12.
9. Choudhary N and Tharani L, "Preventing Black Hole Attack in AODV using timer-based detection mechanism," 2015 International Conference on Signal Processing

and Communication Engineering Systems, Guntur, pp. 1-4, 2015

10. E. O. Ochola, L. F. Mejaele, M. M. Eloff and J. A. van der Poll, "Manet Reactive Routing Protocols Node Mobility Variation Effect in Analysing the Impact of Black Hole Attack," in SAIEE Africa Research Journal, vol. 108, no. 2, pp. 80-92, June 2017.
11. Yasin, Adwan and Mahmoud Abu-Zant. “Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique.” Wireless Communications and Mobile Computing 2018 (2018): 9812135:1-9812135:10.
12. N. Jaisankar, R. Saravanan, K. DuraiSwamy, "A novel security approach for detecting black hole attack in MANET", Information Processing and Management Communications in Computer and Information Science, vol. 70, pp. 217-223, 2010.
13. N. Sharma and A. Sharma, "The Black-Hole Node Attack in MANET," 2012 Second International Conference on Advanced Computing & Communication Technologies, Rohtak, Haryana, pp. 546-550, 2012
14. M. Umar, A. Sabo and A. A. Tata, "Modified Cooperative Bait Detection Scheme for Detecting and Preventing Cooperative Blackhole and Eavesdropping Attacks in MANET," 2018 International Conference on Networking and Network Applications (NaNA), Xi'an, China, pp. 121-126, 2018.
15. Vikash Kumar "Prevention of Black Hole Attacks in MANETs" International Journal of Engineering Trends and Technology Vol. 61, Issue. 3, pp. 166-170, 2018.
16. Imran, M., Khan,F.A., Abbas, H., Iftikhar,M. Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks. Security in Ad Hoc Networks (SecAN) Workshop, 13th International Conference on Ad-Hoc and Wireless Networks (ADHOC-NOW), Benidorm, Spain, June 22-27, 2014.
17. S. Dhende, S. Musale, S. Shirbahadurkar and A. Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs," 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2017, pp. 2391-2394.
18. Tiruvakadu, D.S.K., Pallapa, V. Honeypot Based Black-Hole Attack Confirmation in a MANET. Int J Wireless Inf Networks **25,** 434–448.
19. Gayathri A and Narayanasamy P, “Security in MANET’s by using Detective Signature Techniques”, Journal of Computer Science, Vol.11, Issue 3, pp. 526-533, 2015.