International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Utilization of Energy Consumption Metric to Detect Black Hole Attacker in DSR Routing Protocol

R. Saranya, R.S. Rajesh

Abstract: ***A Mobile Adhoc Network (MANET) is a self-organized system comprised of multiple mobile wireless nodes. They do not require the existing network infrastructure. Autonomous telescopes can change freely and inadvertently in a network that can establish a dynamic network temporarily, and these networks can often change their appearance. Due to the openness in network topology and the absence of centralized administration in management, MANET is vulnerable to attacks from malicious nodes. Therefore, security is a major issue in MANET, which drastically reduces network performance. Several trust parameters such as packet delivery ratio, packet dropping ratio, etc are used for detecting the malicious node attack in MANET. Among these, this paper uses the energy as the trust parameter for detecting the malicious node. The energy reduction ratio differs from the normal node and attacker node in MANET. Hence, the main aim of this paper is to find the Normal Energy Reduction Ratio (NERR) and Attacker Energy Reduction Ratio (AERR). These two values are used for differentiating the normal node and attacker node in MANET. For routing, this paper uses the Dynamic Source Routing (DSR) Protocol.***

Keywords: Mobile ad hoc network (MANET), DSR Protocol, Energy Reduction, Attacker Node

I. INTRODUCTION

Wireless networks can be classified into the network with infrastructure and networks without infrastructure. MANET belongs to the last group where the mobile node can acts as a host and a router when forwarding another node's package. MANETs are easy to use and strong in nature, so they can be used in geographical or mainland areas such as battlefields in disaster management, indoor communication, and dynamic communication environment. MANET's mobile number is connected via a wireless channel and messaging is a major concern. There is no router or access point in wireless mobile ad hoc network (MANET). The transfer of data between nodes is achieved with the help of multiple hops. Each mobile node acts as a host and as a router to create a path. When a node of a source intends to transfer the data to the target node, the package is passed through the intermediate node, so the quick search and creation of the path from the source to the destination is the main question of the munitions. Currently, available MANET transport protocols are classified as main types in Route Reaction and Reaction protocols.

Standard transmission protocols such as the DSR are designed regardless of the MANET safety constraints. In this way, MANETs, based on DSET, may be vulnerable to various types of attacks such as black hole attacks, worm's attacks, and cyber-attacks [1]. In this article, our focus is on black hole attacks. The Blackhole Attack [2] is an attack where every packet on the network is redirected to a special node (called a red node). When the packets reach this point of evil, they just disappear, is said to have disappeared into the black holes in the universe. In fact, the black hole node represents as the target node by sending a packet response packet to a source node that initiates the path detection and thus breaking the packets of the source node. The black hole node has two properties. First, the node takes advantage of a dedicated transmission protocol, such as the DSR, to properly propagate to the target node, even though the path is fake, with the intention of blocking the packet. Second, the node uses the captured package. This type of attack is potentially harmful and can result in huge network damage.

II. RELATED WORK

Black Hole attack comes under a denial of service attack type which uses the vulnerability of packet delivery in routing protocols to spread the shortest route to the node where it wants to infect. The attack aims to modify the transmission protocol, so traffic through a special node controlled by an attacker. Black holes can be caused by bad intent nodes. Techniques that are asked to discover and remove the black holes in the literature are described as follows: Shalini Jane [6] asked to find and remove dangerous nodes, which started with black hole attacks. In this work, a malicious node is detected and removed between the two block changes, ensuring end-to-end authentication. The Send Yield node starts up to the target key before initiating each block to alert it to the incoming data block. The flow of traffic is checked by the neighbor of each node in the path. After the end of the sending center, the node sends an acknowledgment via an active message containing the package data numbers obtained by the target node. In this process, the process of detecting and removing malicious nodes by gathering responses from nodes, controls, and networks.

Manuscript published on 30 September 2019
* Correspondence Author
R. Saranya*, CSE department, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India. Email: saranya.shantha@gmail.com
R.S.Rajesh, CSE department, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India. Email: rs_rajesh1@yahoo.co.in

Deng, Li, and Agrawal [4] have requested black hole attacks that protect against AODV transmission. In this work, the route path is obtained from one of the intermediate nodes in the official, the other path is transmitted from the resulting nodes to the next node of the mean node in the path. This research will eliminate black hole attacks by a single striker, but it also fails in the event of a gray attack with a hole.

Chang Wu Yu et al. [3] Requested DCM (Distributor and Collaborative Mechanism) to address Blackhole attacks. In this work, he made many steps to evaluate. Each node on the network has an evaluation table. Package information is used to evaluate erroneous nodes. For suspicious nodes, the scanning node detects the basis for setting the black hole. The target node opens the packet to search for the cooperative node. If the value of the check is positive, then the node is deemed to be a normal node. Otherwise, the node opens a Procedure for Co-Pro and relates to the dissemination and notification to all neighbors using the module to participate in the decision-making process. Hesiri Weerasinghe [5] has proposed Blackhole attacks together based on a solution that defines a safe route between sources and destinations by identifying and closing black hole markets to increase accuracy. This algorithm uses a method to identify several black holes that work together as a team to launch a black hole attack. This job introduces a list of information transmissions (DRI) and monitoring each other through additional requests and additional responses.

Tamilselvan [7] has proposed a Channel Discovery Approach (CAA), which has proposed two strategies, overseeing lost and hoping for traffic. Each node in the path of forwarding observes neighbor's behavior from past concrete paths and subsequent paths to find invalid nodes. These nodes evaluate the behavior of their neighbors by comparing two-level observations for detection known as the degree of observation and loss rates. With this method, each node in the relay path should control both its neighbors in the currents and the water through an impartial look that causes the loss of energy in each node. Given that this method does not use any non-controllable checks from the node above in the path of the source, the node in the path forward observes the behavior of other nodes via query requests and response.

Lee et al. [8] two different messages were requested, such as CREQ and CREP, to detect black hole attacks. The central node in addition to transferring RREPs to the output node sends CREQs to its next node to the target node. If it does, then sends CREP to the source. After getting the CREP Comparison Source Node shown in RRE. If both are the same, then the source is correct. In [9], Shurman et al. Request a node source to wait until the arrival of the RREP package from the above two nodes. In many RREP lists, the node source checks for general terms. If at least one jump is common, the root node is considered safe. In [10] referral-based associations that should be implemented in the DSR protocol to increase security. The purpose of this scheme is to detect harmful nodes through specific association criteria between two nodes.

In [11], Pirzada and McDonald's presented a methodology for improving the DSR protocol. They provide methods of trustworthy gate deployments to enhance the DSR protocol. This scheme determines the number of dangerous nodes in the network and uses trusted gateways to avoid changing packet data. In [12] all RREP packages are required by the middle node, send to the next hive. After receiving this RREP package, the core source sends additional requests (FREQ) back to check if the route is safe. If the average node responds from FREP in direction of the destination, the source is intended to make the path safe. In [13], the author analyzed the black hole attacks and indicated that the harmful nodes had to raise enough numbers to persuade which node paths were provided. In this paper, the author has proposed a statistical irregularity detection scheme to detect black hole attacks by comparing the target order number of the received RREPs. In [14] the Intrusion Detection System (IDS) is an important technique used to prevent attacks against security threats. Intrusion Detection is the process of detecting black hole attacks by previous actions. This article [15] presents the proposed black hole scheme in the "Blackhole Attack on the DSR (DBA-DSR) Network". The black hole problem before the actual navigation mechanism was started using a fake RREQ package to track the dangerous tips.

The majority of black-hole removal techniques discussed in this section find and delete black hole attacks based on techniques such as channel detection and trust-based methods. The above technique is vulnerable to various issues including tolerance, error, loss of packages, denial of service, and network shutdown. Therefore, the limitations of the existing Black Hole attack techniques can be guidelines for expanding or enhancing the technical aspects of transmission. So the focus of this article is to locate and remove the black hole in the secure data path between the MANET network router numbers.

III. DYNAMIC SOURCE ROUTING PROTOCOL

DSR protocol consists of two mechanisms that work together to allow for the detection and maintenance of external routes in the Adhoc Network: Path Detection is the mechanism that the node S wants to send the packet to the target D receives the source to D Route lookup is only used when S tries to send packets to D and does not know the path for D.

Route Maintenance is a mechanism that S node can detect when using the external route to D if the network is changed so that it cannot use its path to D when the route link is no longer available. When path support shows a broken path source, S may use other routes known to know about D or return to path detection to find new routes. Street support is only used when S actually sends packets to D. Path access and path maintenance work as required. Unlike other protocols, the DSR does not require a temporary block of any type at any network level. For example, the DSR does not use any periodic fixes, contract status, or neighborhood finder packages, and does not rely on these features from any of the major protocols on the network.

This is the whole behavior and the lack of periodic activity allows the number of costs generated by this package, the DSR can be scaled to zero, all at the node, with respect to the station, with respect to any and all that is needed for the official Relationships today, have already been found. As the boot node moves a lot of changes or times of storage of pattern relationships on the street package DSR, only scaling is necessary to trace current route paths being used. In response to the single opening of the path, nodes can learn and caches many paths for each goal.

This allows changes in the reactions to this path to be as far from the routing node can encounter another caching target if one of the routes used has failed. The caches of these roads also avoid the need to apply this roadmap every time the official user interrupts this.

A. ROUTE DISCOVERY

When an S node creates a new package for another intuitive D and put in the header of the route, the package source gives the order of hops that this package must be a way to D Normal S will get the proper source. Finding a route for the path has already learned, but if its cache is not found then it will initiate a protocol opening to find a new way Dynamic D in this case, the S is called Initiative and Target D, of Detection. For example, Figure 1 shows a path, in which a node tried to find the path to the node initiating the discovery of a path and sends a message with ROUTE REQUEST that is received by all the nodes which are currently under a wireless transmission. ROUTE Correspondence identifies the source and destination of the navigation path and only the first request ID. Each railway program also contains entries with addresses of each intermediate node through the Path Response Rules. This item is placed on an empty list by the emulator editor.

When another node becomes a way, if this is the purpose of the spreading path, it returns a message that guides the path that provides a copy of the accumulated road to the proposed path. When the initiative receives a response to the flight path, it caches in its official cache for the use of future routes for that purpose. Otherwise, if the node accepts the request, see Roque another message from ROUTE, this initiative generates the same effect of the request, or if it finds that its own address is already entered in this record of 'To ROUTE' then it will be rejected.

Otherwise, the entity shall add its own address in the path record in the message and send it through a local broadcasting pack (with the same ID on the request). Returning Responsibility the path to the origin of a roadmap, such as an e-nonsense return to one of Figure 1, the normal node will check its caching path to be a return path if it is found, then it will be used as a source for the ROUTE RESPONSE package. Otherwise, it may make its e-turn route to a node, but to avoid the infinite possible detection of the path response, it must replicate its message-response to the node.

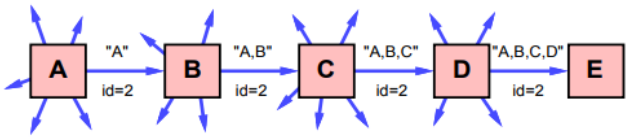

Fig. 1. Route Discovery example: Node A is the initiator, and node E is the target

B. Route Maintenance

When a package originates or sends by a source, each node that sends packets is responsible for verifying that packets are received from the hip later on the source path. Packages are forwarded (up to the maximum of attempts) until the receipt of the receipt. For example, in the image shown in Figure 2, Node A generates the E-Package using the external path through the average node B, C and D. In this case, Node A is responsible for receiving packets in A-B. B is responsible for getting in C, Node C is responsible for Receipt D and D have the final task of receiving the target E. Receiving the receipt in most cases can be provided Free to DSR or existing standard parts of the MAC protocol that will be used.

Without these authentication mechanisms, the node that dispatches the packet may be limited in the header of the packet to request confirmation of a specific DSR program back to back. This software specification is generally sent directly to the sending node, but if the connection between these two nodes is unique, the software specification can cross the multipath. If the package is included several times and does not recognize, then this node returns an error message to the path of the sender of the original file that determines the connection that the package cannot forward.

In Figure 2, if C does not send packets to the next Jump, then C returns the path error to A, indicating that the current C to D link is "corrupted". A link from her cache; the repackage of the original packet is the function of a high-layer protocol such as TCP. To send, like retransmission or other packets to the same direction, if A has a cached path on another route, so that it can send the package using the new route immediately. Otherwise, you can reopen it for that purpose.

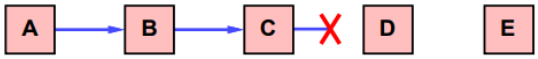

Fig. 2. Route Maintenance example: Node C is unable to forward a packet from A to E over its link to next-hop D.

C. Energy issues for DSR

- The network load created by the DSR's input algorithm still leaves the lost power amount.
- Route Request (RREQ) creates a network-based control pack that monitors the speed of the internet and uses it to access the network if they are not managed.
- This protocol will not be effective on large networks because of the package costs that will continue to increase as the diameter of the network increases.

D. NERR and AERR Calculation

In this section, the malicious node attack in MANET is detected by finding the Normal Energy Reduction Ratio (NERR) and Attack Energy Reduction Ratio (AERR). This ratio values are calculated from the normal node and attacker node in the various time interval. First, note the initial energy of all node as E1 and then send the number of packets at the time interval T1 to all nodes. After sending the packets to calculate the energy value of all nodes and note as E2. Then find the energy consumption at the time T1 using $EC_1 = \frac{E_1 - E_2}{T_1}$. As well as note the energy of all node at time T1 as E2 and then send the number of packets at the time interval T2 to all nodes. After sending the packets, the energy value of all nodes is calculated and note as E3. Then find the energy consumption at the time T2 using $EC_2 = \frac{E_2 - E_3}{T_2}$. And then find the Energy Reduction Ratio (ERR) $= \frac{EC_2}{EC_1}$. Repeat these process for several time intervals and find the ERR values and average them to find the final ERR value.

This ERR value is calculated from the normal nodes it is considered as NERR value otherwise it is considered as the AERR. Then these values are used as the threshold for finding the attacker node.

IV. EXPERIMENT EVALUATION

The proposed system is implemented using Network Simulator (NS2). In the simulation experiments, several parameters are used. They are listed in the table given as follows.

Table-1: Different Parameters Used In the Simulation

No of Nodes	50
Area Size	1000m x 1000m
Target Size	[500,500] x [500,500]
Simulation Duration	150 seconds
Queue Limit	20
Queue Size	100
Packet Size	552 Bytes
Packet Interval	2
Communication Range	30 m
Buffer Size	20 packets

IV. EXPERIMENT RESULTS

This paper study the energy reduction ratio of the normal node and attacker node for the different number of nodes. The results are captured and showed in Fig. 3. In this study, the percentage of malicious nodes varies from 0% to 10% for all network. The maximum speed of nodes is set to 20 m/s. From the above Fig.3, it can be observed that NERR value ranges from 70 to 80 and AERR value ranges from 45 to 70.

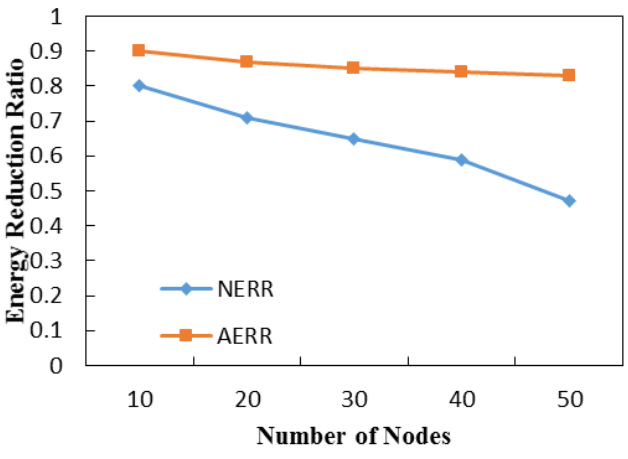

Fig. 3. Energy Reduction Ratio of Normal Node and Attacker Node for different Number of Nodes

This paper study the energy reduction ratio of the normal node and attacker node for the different number of nodes. The results are captured and showed in Fig. 3. In this study, the percentage of malicious nodes varies from 0% to 10% for all network. The maximum speed of nodes is set to 20 m/s. From the above Fig.3, it can be observed that NERR value ranges from 70 to 80, and AERR value ranges from 45 to 70.

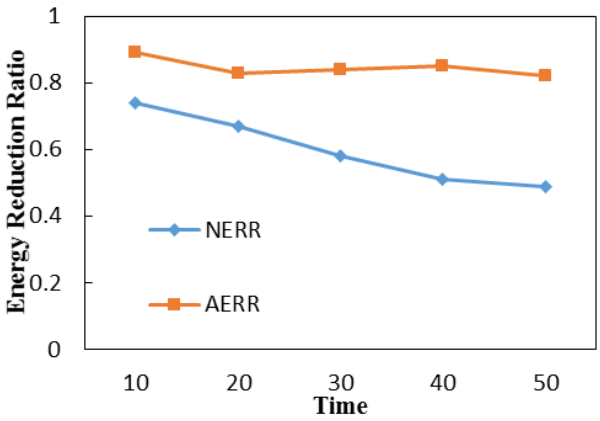

Fig. 4. Energy Reduction Ratio of Normal Node and Attacker Node for the different time interval

This paper study the energy reduction ratio of the normal node and attacker node for the different time interval. The results are captured and showed in Fig. 4. In this study, the percentage of malicious nodes varies from 0% to 10% for all network. The maximum speed of nodes is set to 20 m/s. From the above Fig.3, it can be observed that NERR value ranges from 70 to 80 and AERR value ranges from 45 to 70.

V. CONCLUSION

In this paper, the malicious node attack in MANET is detected by using the Energy Reduction Ratio(ERR).To differentiate the normal node and attacker node in MANET this paper calculates the NERR value and AERR value at a different time interval. From the experimental result, it is clearly shown that the NERR value ranges from 70 to 100 and the AERR value ranges from 10 to 70. The energy as the trust parameter for detecting the malicious node. These two values are used as the threshold value for differentiating the normal node and attacker node in MANET.

REFERENCES

1. R. H. Khokhar, A. N. Ngadi, A. Mandala, “A review of current routing attacks in mobile ad hoc networks”, Intl. Journal of Computer Science and Security, pp. 18-29, vol. 2, Issue-3, 2008.
2. E. M. Royer, C.Toh, “Review of current routing protocols for ad hoc mobile wireless networks”, IEEE Personal Communications, 6(2), pp. 46-55, 1999.
3. C-C Chiang, H-K Wu, W .Liu, M.Gerla “Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel”, In Proceedings of IEEE SICON, pp.197–211, 1997.
4. H. Deng, W. Li, and Dharma P. Agrawal, “Routing Security in Ad Hoc Networks,” IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, pp. 70-75, October 2002.
5. HesiriWeerasinghe and Huirong Fu, Member of IEEE, “Preventing Cooperative Black Hole Attacks in Mobile Ad-hoc Networks”, Simulation implementation and evaluation, Vol. 2, No.3, July 2008.

6. Shalini, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by dynamic learning method", International Journal of Network Security", Vol.5, No.3, pp. 338-346, 2007.
7. Tamilselvan, L.Sankaranarayanan, "Prevention of black hole Attack in MANET", International Journal of networks Network Security, Vol.3, No.5, May 2008.
8. S.Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto, "Detecting Black Hole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol. 5, No. 3, 2007.
9. Nisha P John, Ashly Thomas, "Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review", International Journal of Innovative Research and Development 1, 232-245.
10. N.Bhalaji, Dr.A.Shanmugam, "Association between Nodes to Combat Black Hole Attack in DSR Based Manet",978-1-4244-3474-9/09/$25.00 ©2009 IEEE.
11. Asad Amir Pirzada, Chris McDonald, "Deploying Trust Gateways to Reinforce Dynamic Source Routing", 2005 3rd IEEE International Conference on Industrial Informatics, (INDIN '05), Aug. 10-12, 2005
12. Akshat Jain, Shekher Singh Sengar, Vikas Goel "Colluding Black Holes Detection in MANET" (IJERT), Vol. 2 Issue 1, January- 2013 ISSN: 2278- 0181
13. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", (IJNS), Vol.5, No.3, Nov. 2007
14. Yibeltal Fantahun Alem, Zhao Cheng Xuan," Preventing Black Hole Attack in Mobile Adhoc Networks Using Anomaly Detection", 978-1-4244-5824-0/$26.00 c 2010 IEEE
15. Isaac Woungang," Detecting Blackhole Attacks on DSR-based Mobile Ad Hoc Networks", 978-1- 4673-1550-0/12©2012 IEEE

AUTHOR PROFILE

R. Saranaya received her B.E. degree from Anna University, M.E degree from Manonmaniam Sundaranar University in 2011 and 2013 respectively. Currently, she is working towards a Ph.D. in Manonmaniam Sundaranar University, India. Her research topics are wireless networks, network security, and Network Routing Protocol.

Dr. R.S. Rajesh received his B.E and M.E degrees in Electronics and Communication Engineering from Madurai Kamaraj University, Madurai, India in the year 1988 and 1989 respectively. He is currently the Professor and Head of Department of Computer Science and Engineering, Manonmaniam Sundaranar University where he earned his Doctorate degree in the field of Computer Science and Engineering in the year 2004. He has 22 years of PG teaching experience. He has published 100 articles in leading international journals. His research areas include Vehicular Adhoc Networks, Wireless networks, Digital image processing, and Pervasive computing..