International Journal of Emerging Science and Engineering (IJESE)
ISSN: 2319–6378 (Online), Volume-11 Issue-4, March 2023

Neighbour Node Ratio AODV (NNR-AODV) Routing Protocol for Wormhole Attack Detection in Manets

M V D S Krishna Murty, Lakshmi Rajamani

Abstract*: *This paper aimed at the detection of wormhole attack and proposed a new method called as Neighbour Node Ratio Adhoc On demand Distance Vector Routing (NNR-AODV). NNR-AODV is an extended version of the traditional AODV routing protocol. The proposed NNR-AODV calculates the neighbour node count for every node and based on that it will decide whether the wormhole is present or not. Furthermore, NNR-AODV is able to detect both external and internal wormhole attacked nodes. Also, NNR-AODV derived a Neighbor node Threshold value which is based on the cumulative distances between nodes present in the wormhole attack. For experimental validation, we have accomplished an extensive simulation and the performance is measured through Number of bogus links, Detection rate, False positive Rate, Packet delivery ratio and Packet loss ratio. The obtained results have shown superior performance in the detection of wormhole attacks than the existing methods.

Keywords*: *Wormhole, Neighbor Node Threshold, Bogus Links and Node Degree.

I. INTRODUCTION

From the past few years, rapid progress in the development of Mobile Ad Hoc Networks (MANETs) has encouraged different wireless applications that can be employed in different areas viz. Entrainment, Education, Military, Emergency services and Collaborative computing [1]. Due to the special characteristics of MANETs viz. independent infrastructure and self-organizing nodes, MANETs have become an ideal choice to use in information sharing and communications. Thus, the mobile nodes of MANET can execute both for routing and hosting. In the case of routing, they work as relay nodes and forward the data of a node to its destination through standard protocols. However, the major issue in MANETs is their mobility which introduces several serious constraints on network lifetime, quality of service and security [2-4]. Due to the nature of decentralization and openness of MANETs, the mobile nodes are not reliable to constrain the membership. The mobile nodes are susceptible to different attacks [5] when those who try to compromise the node and force it to misbehave. Based on the nature of attack, they ranges from passive eavesdropping to serious battery draining. Some more attacks are there which aim at data tampering and traffic analysis through eavesdropping. In general, the attackers mainly concentrate on the resources of mobile nodes like bandwidth exhaustion, battery draining and data manipulations etc. Based on the mode of attack, they are categorized as external mode attacks and internal mode attacks [6]. The former attacks concentrate on the manipulation of routing information that propagates between mobile nodes in the network. They inject erroneous data and try to disturb the original behavior of network. An example for such kind of attack is worm-hole attack (WHA) in which a routing loop is established by the creation of a worm-hole node. Next, the internal attacks mainly target at compromising internal nodes. They distribute false data and try to disrupt the data flow. Sybil attack, grayhole attack and blackhole attack are the best examples to such kind of attacks.

Wormhole attacks are the most severe and sophisticated security threats to the MANET routing protocols where malicious nodes are placed strategically to distort the network topology and tunnel packets selectively using the false established routes [7], [8]. Wormhole detection and prevention are very challenging issues [9], [10]. The wormhole attacks can be executed by external nodes (who only forward packets and do not process the cryptographic data) or by internal nodes (the compromised nodes inside the network who process packets like other normal nodes) [11]. The internal attackers are more dangerous and difficult to detect. However, Chen *et al.* [12] hold the view that the wormhole attack is a typical external attack. Moreover, majority works of literature pay excessive attention to the external wormholes but ignore internal wormholes which are also common in MANETs.

This paper proposed a new method called as Neighbour Node Ratio AODV(NNR-AODV) routing protocol to prevent the MANETs from wormhole attacks. The proposed NNR-AODV detects both the external and internal wormhole attacks effectively. NNR-AODV derived a metric called as neighbour node threshold, which avoids the attack by performing wormhole (WH) detections for all nodes in MANETs, thus contributes in improving the accuracy of wormhole detection and saves energy.

Manuscript received on 01 March 2023 | Revised Manuscript received on 14 March 2023 | Manuscript Accepted on 15 March 2023 | Manuscript published on 30 March 2023.
*****Correspondence Author(s)
M V D S Krishna Murty*, Research Scholar, Department of CSE, Jawaharlal Nehru Technological University Hyderabad (Telangana), India. E-mail: mkrishnamurty@gmail.com, ORCID ID: https://orcid.org/0000-0002-4705-3818
Dr. Lakshmi Rajamani, Professor and Head (Retd), Department of CSE, Osmania University, Hyderabad (Telangana), India. E-mail: drlakshmiraja@gmail.com

The remaining paper is organized as follows; section II explores the literature survey on wormhole detection methods. Section III explores the details of proposed NNR-AODV. Section IV explores the details of simulation experiments and the final section concludes the paper.

II. LITERATURE SURVEY

In this survey, we have explored different earlier methods those were mainly aimed at the detection of wormhole attacks in MANETs.

M. Tahboush and M. Agoyi [13] aimed at the identification of both external WHA and internal WHA and proposed a hybrid WHA detection algorithm. They suggested counting packet delivery ratio, hop count based Round Trip Time (RTT) for external WHA detection. For internal WHA detection, they suggested to compute communication range between consecutive nodes in network. This approach didn't use any external middleware and hardware. Also it reduced the energy and delay by avoiding WH loads in the network. They used NS-2 Simulator for experimental validation and used performance metrics namely end-to-end delay, average energy consumption, packet delivery ratio and throughput. They used AODV as a base reference protocol.

H. Ghayvat et al [14] proposed a secure AODV by introducing a digital signature to detect and mitigate WHA in MANETs. This approach suggested computing the tunneling time taken by the tunnel for the analysis of WH behavior. Then, a threshold is decided and based on these two values the node is decided whether it is WH not or not. Further, they applied hash-chain and digital signature algorithm for the mitigation of WHA. S. Tripathi [15] analyzed the repercussion of WHA in MANETs through DSR and AODV with varying number of WH tunnels.

M. Shukla and B. K. Joshi [16] proposed to compute two parameters namely data rate and receiving time and formulated a trust metric to identify the WHA in MANETs. S. Majumder and D. Bhattacharyya [17] aimed at WHA prevention and avoidance and proposed a statistical method based on absolute deviation (AD). AD correlation and covariance take very less time to detect WHA as the original path takes more time than the fake tunnel and the computation of the time taken for delivery helped in the identification of WHA.

S. N. Ghormare et al. [18] aimed at the prevention and detection of WHA in Wi-Max based MANETs through AODV. In this attack model, the compromised mobile node puts the packet in some other location and then forwards it to another compromised node which lies away from tunneling. A. Bhawsar et al. [19] calculated trust in AODV routing protocol for the detection and prevention of WHA. This approach suggested a multipath selection to find the best routing path. All the available paths are tested for WHA and finally one path is selected which has no WHA node.

N. Al-Bulushi et al.[20] analyzed the effect of two types of attacks such as WHA with mobile nodes and WHA with static nodes. Here, the compromised nodes are assumed to be either static or mobile. They used two routing protocols namely optimized link State Routing (OLSR) and AODV for routing process.

M. Prasad et al. [21] employed a machine learning algorithm for WHA detection. They executed their methodology in three phases. In the first phase they simulated network with multiple WH tunnels. In the next phase, they executed packet attributes characterization and based on that selection of features is done. Then ,they performed data collection and aggregation from large volume of data set. In the final phase, they applied machine learning algorithm for WHA detection.

S. Sharma and R. M. Sharma [22] proposed a hop count model assisted routing protocol called as Extended Prime Product Number (EPPN) to find WHA in MANETs. They computed the hop count of an active path between source and destination and integrated in AODV protocol. Based on the obtained hop account value WHA is detected if it is more than the received hop count. H. As'adi e al. [23] proposed to calculate two statistical parameters viz. number of neighbours and number of new neighbours for every node in a decentralized manner. This mechanism suffers from less delay and also it won't create extra traffic overhead in the network.

Based on the fact of reduced WH tunnel length than the original path length, M. Rmayti et al.[24] proposed a new WHA detection model in which a mobile node can check whether a presumed shortest path has WH node or not. K. N. Venkata Ratna Kumar et al.[25] computed RTT and sequence number in their proposed Cluster Based Algorithm (CBA) for WHA detection. They focused on both in-band and out-band WHA detection. To differentiate between no attack and attack routes, they used CBA to estimate the threshold of RTT.

F. A. F. Alenezi et al. [26] proposed a new WHA detection mechanism called as SDN based WH analysis using the neighbour similarity (SWANS) for software defined MANETs. In a centralized SDN controller, the proposed method analyses the neighbours count similarity. The proposed approach optimally detects WHAs without using specific location information and also without causing any co-ordination and communication overhead. Further, the SWANS also reduced the false negatives and false positives those were due to the Link Layer Discovery Protocol (LLDP) vulnerability.

B. Bhushan and G. Sahoo [27] accomplished time synchronization and location information to detect WHA in MANETs. They also exploded packet leashes for WHA detection. Y. Sun and Y. Chen [28] proposed anomaly detection algorithm based on mean shift and median absolute deviation for WHA detection in MANETs. This method detects WHA based on the abnormal forwarding number and abnormal time in single hop between nodes. Also, this approach has very less overhead and does not require any special hardware for the synchronization of time. R. Shukla et al.[29] proposed trust and energy aware secure routing protocol (TESRP) to provide security against WHA. This approach is considered as one of the best approaches but it was not able to identify WHA. Hence the authors used TESRP with sequence number for security provision in network from WHA.

K. D. Thilak et al.[30] proposed to calculate the circulated discovery against wormhole in remote organization coding framework. Initially they proposed a centralized strategy to detect WHA and its accuracy is explored rigorously.

Adversary nodes are identified on both sides of communication and discarded from the network. They brought a bundle Miss Fortune adversary nodes for avoiding the loss of packets and data transmission takes place after the separation of nodes from network. After separating advisory nodes between source and destination nodes, the packets are retransmitted. They selected the shortest path that was not affected by WHA and packet transmission is attempted between source and destination successfully and effectively.

III. PROPOSED APPROACH

3.1 Overview

NNR-AODV aims at the detection of wormhole attacks in MANETs. Wormhole attacks are usually initiated by the conspiracy of two malicious nodes. The two nodes are located at the ends of the network far apart, and their configuration information will not appear in the routing table, so they are hidden from normal nodes. When the data is forwarded, the wormhole node transmits packets to the colluding node through a private tunnel, and the colluding node broadcasts the received packets to its neighbor. Thereby the normal transmission of data is disturbed, and then the network performance is affected.

3.2. Neighbor Node Ratio (NNR)

Verifying all the nodes in a network about their trustworthiness is time consuming and battery energy consuming process. Since, only few nodes have the ability to get compromised by WHA, they only needed to be determined. In general ,the attacks raise the network connectivity and hence there is an obvious rise in the number of neighbours. Hence, the neighbour number of nodes which has an impact of WHA is more than a node that was not in the WHA scope. Hence,we have proposed a threshold which was used to compare the neighbour number of all nodes in the network to determine the suspected nodes which have the scope of WHA. The threshold is calculated according to the following equation.

$$NNR_T = \frac{N\pi r^2}{S} \qquad (1)$$

Specifically, the suspected nodes identification is done as follows; 1. Every node knows its neighbour nodes after their deployment in network. 2. Then, each node calculates NNR and the average NNR of all of its neighbour nodes. 3. The NNR is compared with NNR_T to determine whether the requirement of detection process is necessary or not.

Among the determined suspected nodes, the External WHA(EWHA) detection mechanism is applied on the nodes who are direct neighbours and Internal WHA(IWHA) is done on the remaining nodes that have common neighbour nodes.

3.3 Wormhole Detection

At this phase, WHA detection mechanism is divided into two tasks viz. EWHA detection and IWHA detection. The details of these two mechanisms are explored in the following subsections.

3.3.1 External Wormhole Detection

EWHA detection must be applied on the suspected node pair who is in direct communication with each other. The main theme of EWHA detection is comparing the differences in hop count between exclusive neighbours of target nodes.

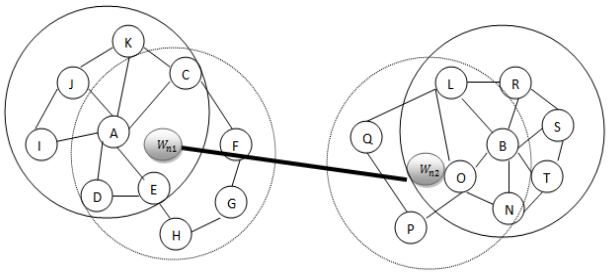

Figure. 1 External Wormhole Attack

In Fig.1, node A and node B assumes that they are neighbours and the nodes within the communication range of W_{n2} are mistakenly assume that they are one hop neighbours of nodes within the communication range of W_{n1}. Hence, the neighbour nodes set of node A is denoted as $N_A = \{B, C, D, E, I, J, K, L, N, O, P, Q\}$. Similarly the neighbour nodes set of node B is denoted as $N_B = \{A, C, D, E, F, G, H, L, N, O, R, S, T\}$. Based on these two neighbours set, the common neighbour set is obtained as $N_A \cap N_B = \{C, D, E, L, N, O\}$. Then the exclusive neighbour set of node A is obtained as $N'_A = N_A - N_A \cap N_B - \{B\} = \{I, J, K, P, Q\}$. As it was known that for node A ,in its exclusive neighbour set N'_A, the max hop count between any two nodes is one. However, based on this fact, it is seen that $\{I, J, K\}$ and $\{P, Q\}$ are located much away from each other and the original hop count is larger than 1.

Based on the above exploration, nodes can be chosen who have more than two exclusive neighbour numbers between any node pair and new links are mentioned among the set of exclusive neighbours. These must bypass the other neighbor's node. Then, the hop counts of these new links are calculated and compared with the WH threshold to detect the presence of attacked nodes. Consider a node A from the pair of node A and B, then mention that any of the node link in the exclusive neighbour set $\{I, J, K, P, Q\}$ of node A must

bypass the nodes in the communication range of node B, i.e., the neighbour node set of node B.

It is assumed that the nodes A and B have a EWH between them and upon exceeding the hop count from WH threshold, i.e., the link from node to node I to node P. Then the nodes A and B discarded them from their routing tables and propagate the removed neighbour nodes information to the network. If such a situation is not incurred, then it can be stated that there is no WHA.

3.3.2 Internal Wormhole Detection

After identifying the WH nodes from the suspected nodes, the links associated with WHs are much less than the WH threshold and they are successfully detected and discarded from the network. But there exists some EWHs and IWHs whose links or shorter and they are not identified at EWHA detection. Hence IWHA detection takes that responsibility. According to the discussion done above, the IWHA detection must be executed on the remaining nodes those have common neighbour nodes in the suspected nodes list. The major theme of IWHA detection is to activate node pairs in the suspected list those have common neighbours as a proof to hear either the data packets between them are forwarded or not. Initially the pair of nodes that are ready for IWHA detection must get the current verification where their neighbour nodes are not able to forward data at the time of verification such that the prevention can be accomplished. After entering into the monitoring mode, one of the common neighbours in the node pair sends an authentication packet to the node on the other side. If the node on the other side found that it heard irrelevant information then the packets are resent from sender node again.

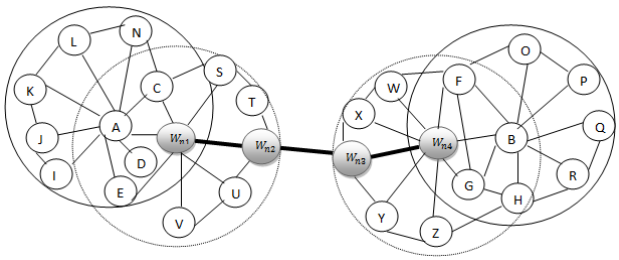

Figure.2. Internal Wormhole attack

As shown in Fig.2, a wrong assumption is made at node A and B about their one hope neighbour relation due to the IWH nodes such as W_{n1}, W_{n2}, W_{n3} and W_{n4}. Node A mistakenly takes the neighbour set as and similarly node B mistakenly take the neighbour set as

$N_A = \{B, C, D, E, G, H, I, J, K, L, N, W, X, Y, Z, W_{n1} \text{ and } W_{n3}\}$

$N_B = \{A, C, D, E, F, G, H, O, P, Q, R, S, T, U, V, W_{n2} \text{ and } W_{n4}\}$. For the determination of link between node A and B, the common neighbour set need to be determined as $N_A \cap N_B = \{C, D, E, F, G, H\}$. This set is used as an evidence for local monitoring. Until they get the right of verification, the common neighbours of node A and B are not able to send the messages. The common node set, i.e., $N_A \cap N_B$ and node A moves into the monitoring state. Then, an authentication packet is formulated by node A by mentioning the address of the destination and sends it to node B. After the packet transmission, node A and the evidence nodes are able to hear three possible types of packets. They are -1) node A's forwarded packet node 2) Node B's reply packet and 3) other node's transmitted packets. Further, there is a chance that some evidence nodes may not receive at least one packet because they might not be real neighbour nodes of A and B.

Initially, for every evidence node, a tag is initiated for the link $A \rightarrow B$ as zero. Upon receiving the packet at any evidence node, it enables the tag $A \rightarrow B$ to one. The packet may be any kind of packet those are mentioned above. On the other hand, upon receiving a overhearing about the forwarding of authentication packet ,the evidence node enables the tag $A \rightarrow B$ to -1. Thirdly, if the evidence node receives any unnecessary and irrelevant data ,then it keeps tag $A \rightarrow B$ as zero. Then, node A receives the tag values from all the evidence nodes and computes the sum , denoted as *s*. Based on the *s* value and the monitoring status updated given by node A, it can determine the presence of IWH between itself and node B. If the reply sent by node B was received at node A within the specified time (denotes the maximum possible communication delay in MANETs), node A assumes that the WH is not there between node A and B whatever the value of *s* is. During the monitoring phase, if node A founds that the packet has been forwarded, it assumes that the WH is there between node A and B whatever the value of s is. If nothing was heard by node A within the stipulated time period, then node A's decision purely depends on the *s* value. For s value value greater than 1, the absence of WH is declared while for *s* value less than 1, the presence of WH is declared. Upon the determination of WH, node A and B discard them each other from their monitoring tables and then propagate updated information to other neighbours.

3.3.3 Wormhole Threshold

For the given two nodes A and B, Figure.3 shows a normal relationship. Assume that the exclusive neighbour set of node A can communicate with all the exclusive neighbour nodes of node B. The locations of two farthest nodes are shown in Figure.4.3. When the data packets sent by node O to the target node D, the possible shortest path is $O-C-E-F-D$ and the length obtained by the summation of d_1, d_2, d_3, and d_4 is less than or equal to communication radius. Then, the path hop count is $l <= 4\left(l = {(d_1 + d_2 + d_3 + d_4)}/{r}\right)$. It becomes $l = 4r$ only when the distance between node A and

Retrieval Number: 100.1/ijese.D25470311423
DOI: 10.35940/ijese.D2547.0311423
Journal Website: www.ijese.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

B is equal to the communication radius. At such condition the path hop count becomes 4.

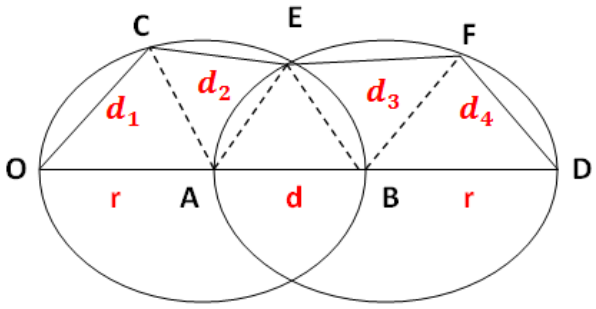

Figure.3 Node Communication model

As shown in the Fig.3,it is seen that if there exists a WH between nodes A and B then the minimum hop count of the reference path established between the exclusive neighbour nodes A and B must be greater than 4. Hence, the WH threshold ε is set as $\varepsilon = 4 + \varphi$. If the hop count for a path established between nodes in N_A' and N_B' is less than WH threshold, then it is declared that there is no WHA otherwise the nodes A and B assume that they are likely to be attacked by WHA. However, such kind of strict declaration may succeed only for some instances. For example, some nodes on the path may have very less residual energy and hence they can't co-operate. In such conditions, the decisions based on just hop count results in larger false positivity. Hence, to reduce such errors, the paths those have more hop count than WH threshold are kept under testing. For such kind of paths, an additional path trust evaluation is carried out.

IV. SIMULATION ANALYSIS

In this section, we have presented the evaluation results of NNR-AODV. First, the experimental setups and the parameters that have an impact on NNR-AODV are shown. Then, baseline methods and performance metrics are presented. Finally, the evaluation and comparison result of NNR-AODV as the parameters change are presented.

4.1 Simulation Setup

Under the simulation setup, initially a random network is created with *N* number of nodes and the network area is considered as 1000*1000 m^2. The creation of simulation set up is done in such a way that the random nature of mobile node could be realized. Means for every simulation, the nodes positions change randomly thereby the neighbor nodes also change. Once the mobile nodes are deployed in the network, every node finds its neighbor nodes based on their communication range. After the discovery, the source node broadcasts route request packet and based on the obtained route replies, a final path is established and then the data transmission starts to destination node. After the completion of data transmission from source to destination, the performance is analyzed through several performance metrics. To analyze the performance of proposed approach, various kinds of simulations are conducted by varying different network parameters. Table.1 shows the simulation set up details.

Table.1 Simulation set up

Network parameter	Value
Number of nodes	30, 40, 50, 60
Network area	1000*1000 m^2
Transmission Range	10% of Length of Network
Node speed	5 m/s to 25 m/s
Data rate	2 to 10 packets/sec
Nodes deployment	Random
Number of Wormholes	2-10
Size of each packet	100 bytes
Simulation Time	200 Sec

4.2 Performance metrics

For the performance analysis, we have considered three performance metrics namely Number of Bogus links, Malicious Detection rate (MDR) and False Positive Rate (FPR). They are measured with varying node parameters such as Node Degree, Wormhole Number, and Neighbor Node Ratio Threshold.

***Node Degree*:** The degree of a node is the number of edges connected to the node, which can also be considered as the average node number per communication range of a node. Eq.(4.2) shows the calculation of *Node Degree*, where r_{max} is the maximum transmission range of nodes, *N* is the total number of nodes, *L* and *W* are the length and width of the network area respectively. When *N* = 40, the *Node Degree* is 12, i.e. there are about 12 nodes in the communication range of a node.

$$Node\ Degree = \pi r_{max}^2 \times \frac{N}{L.W} \times 10 \qquad (4.2)$$

V. RESULTS

Under the results section, the performance of proposed method is analyzed through five performance metrics ; they are - Number of Bogus links, MDR, FPR, Packet Delivery Ratio (PDR) and Packet Loss Ratio (PLR). These metrics are measured by varying different network parameters including wormhole number, node degree, and node count. The obtained results are demonstrated through the following figures.

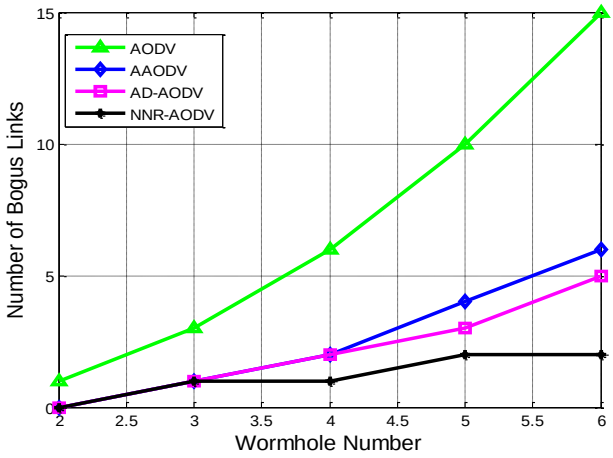

Figure.4 Number of bogus links for varying wormhole count

Retrieval Number: 100.1/ijese.D25470311423
DOI: 10.35940/ijese.D2547.0311423
Journal Website: www.ijese.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Fig.4 shows the impact of wormhole count on the creation of number of bogus links. As the number of wormhole nodes increases in the network, the number of bogus links also increases. Since the presence of a wormhole node in the network tries to establish a bogus and wormhole link, the number of false or bogus links rises linearly. The results shown in Figure.4 shows that the AODV has followed an absolutely linear increment in the rise of number of bogus links for the rise in wormhole count. Compared to the traditional AODV, the remaining methods involve a wormhole prevention mechanism and hence they experienced a smaller number of bogus links than AODV. For instance, at wormhole node count 4, the number of bogus links of AODV is observed as 6 whereas for AD-AODV, AAODV and NNR-AODV, it is 2, 2, and 1 respectively. On an average, the number of bogus links of AODV is observed as 8 while for AD-AODV , AAODV and NNR-AODV, it is observed as 3, 2, and 1 respectively.

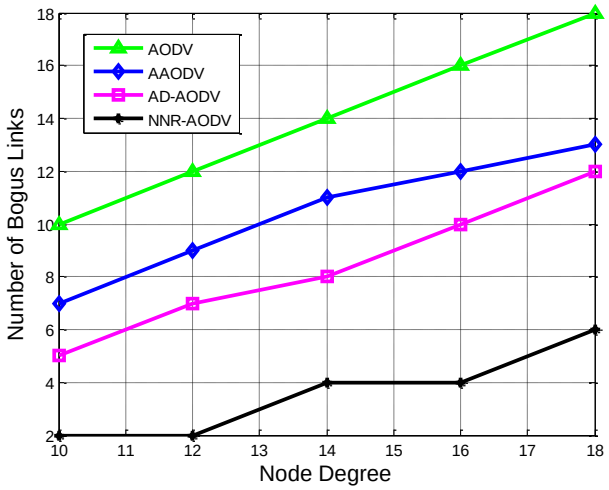

Figure.5 Number of bogus links for varying node degree

Fig.5 shows the impact of node degree on the creation of number of bogus links. Here, the node degree defines the number of nodes within the communication range of a node. The node degree is measured with respect to the communication range of nodes. The node degree is derived with the help of Eq.(4.2) by changing the r_{max} from 10% of network length to 18%. For a wormhole node, the larger node degree reveals the more number of neighbour nodes. As the number of neighbour nodes is larger in number, the wormhole node tries to create more bogus links with them and hence the number of bogus links increases with an increase in the node degree. The results shown in Figure.4 and Figure.5 demonstrate the increasing characteristics of bogus links with the node degree for all the methods. However, the proposed NNR-AODV has experienced a slow increment when compared to the conventional methods as the proposed method adapted a neighbor node ratio which is an important aspect of wormhole attack, thus the NNR-AODV has less number of bogus links. Among the methods, the AODV has experienced more number of bogus links as it won't have any wormhole attack prevention mechanism. On an average, the number of bogus links of AODV is observed as 14 while for AD-AODV, AAODV and NNR-AODV, it is observed as 10, 8, and 3 respectively. The conventional methods cannot effectively detect the external wormhole nodes and also the wormholes with short links. The proposed method detects not only external wormhole nodes but also internal wormholes and performs better than the remaining methods. Next, the number of bogus links of AODV sometimes increases rapidly and sometimes slowly because the nodes are deployed in a random manner and the newly deployed nodes may not get located in the communication rage of wormhole node.

Fig.6 shows the impact of wormhole number on the detection rate and also ,the detection rate decreases with an increase in the wormhole count. With the rise in wormhole nodes, the nodes can establish more number of bogus links and the detection of all such kind of links is a typical issue. Hence, the number bogus links detected are less and results in less detection rate. Even though the detection rate is decreasing, the proposed approach maintained an effective detection rate at all instances of wormhole count. Since the proposed mechanism has applied a neighbour node ratio which is a basic feature of wormhole attack, it can identify the wormhole nodes even at multiple instances. Hence, it gained better Detection rate compared to the existing methods.

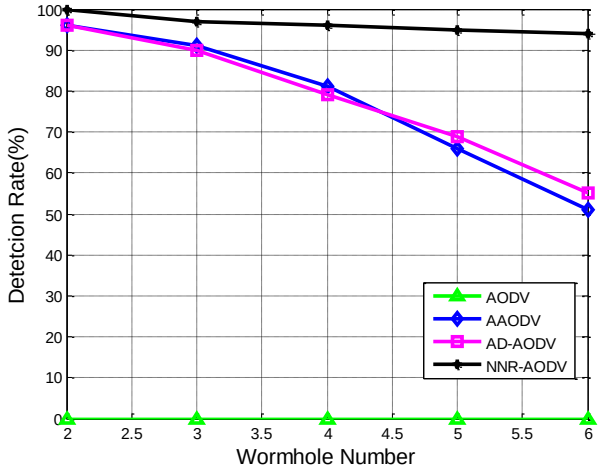

Figure.6 Detection rate for varying wormhole count

The existing methods have shown a fast decrement in the detection rate for an increased wormhole count. AAODV employed Digital signature to prevent the wormhole attacks and used tunneling time taken by tunnel to analyze the behavior of wormhole. For the distant wormhole node pair or normal node pair, the tunneling time is large and in such condition, the identification is tough. Next, AD-AODV applied absolute deviation in time for the identification of wormhole nodes. Compared to neighbor node ratio, the time based measures are less significant and contribute less towards the wormhole node detection. Hence the proposed approach gained more detection rate than the conventional methods. On an average, there is no detection rate for AODV while for AD-AODV, AAODV and NNR-AODV, it is observed as 77.2532%, 78.4230%, and 96.4215% respectively. FPR follows an inverse relation with Detection rate and hence the results shown in Fig.7 are increasing in nature for an increase in wormhole number.

Retrieval Number: 100.1/ijese.D25470311423
DOI: 10.35940/ijese.D2547.0311423
Journal Website: www.ijese.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

In General, the false positive is defined as the node which is declared as wormhole node but in real it is not wormhole node i.e. the node is mistakenly declared as wormhole node. The accumulation of such kind of false positives is used to calculate the FPR. As the number of wormhole nodes increases, the FPR also increases since the detention methods are to identify all the wormhole nodes effectively. However, the proposed method has achieved a better FPR than the conventional methods as it employs a simple and effective NNR mechanism for the identification. As AODV has not got any detection mechanism, it has experienced the maximum FPR. Next, the average FPR of proposed NNR-AODV is observed as 7.2222% while for AD-AODV and AAODV, it is observed as 23.63232% and 26.4578% respectively.

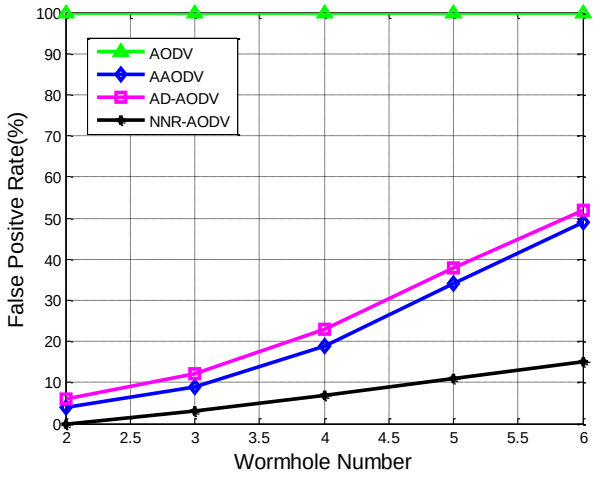

Figure.7 False Positive Rate for varying wormhole count

Upon the occurrence of wormhole attack in MANETs between any source and destination node pairs, they assume that they are just neighbours or one-hop neighbours. Then, the source node forwards the data through wormhole nodes to destination. In such process, upon receiving the data, the wormhole nodes may or may not send the data to destination, or may send only partial data. In both cases, the source node losses some packets and results in less PDR at destination node. In the case of larger node count in the network, the number of bogus links is larger in number and stops to send the data to destination nodes effectively. Due to these reasons, the PDR decreases and PLR increases with an increase in the node count in network. However, the proposed approach is effective in the identification of wormhole nodes in the network, it can help nodes for effective data transmission between source and destination nodes. Hence, the proposed method gained more PDR and less PLR even for larger number of nodes in network. From Fig.8, the average PDR of NNR-AODV is observed as 80.2315% while for conventional methods it is observed as 62.4512%, 57.5555% and 34.7520% i.e. for AD-AODV, AAODV and AODV respectively. Next, from Fig.9, the PLR for the proposed approach is observed as less and its approximate average value is 20.3323% while for conventional methods it is observed as 37.2512%, 42.5277% and 65.3014% i.e. for AD-AODV, AAODV and AODV respectively.

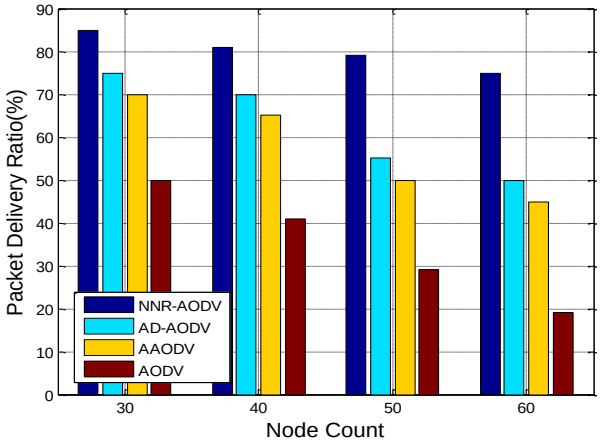

Figure.8 Packet Delivery Ratio for varying node count

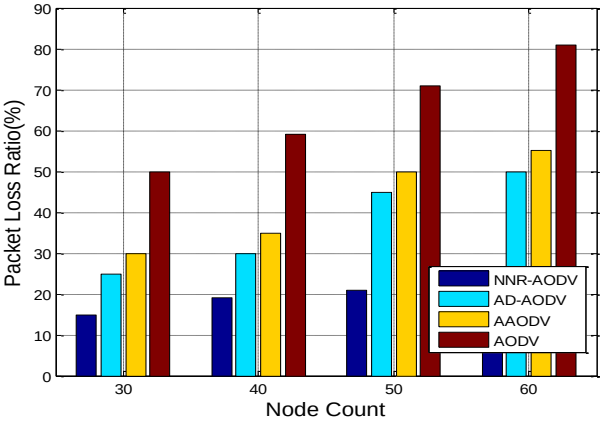

Figure.9 Packet Loss Ratio for varying node count

VI. CONCLUSION

In this paper, we had discussed about the new method proposed for the detection of wormhole attacks in MANETs. The proposed NNR-AODV is simple and light weight in nature and prevents the nodes in MANETs from wormhole attacks. NNR-AODV utilized simple neighbour node calculation for the analysis and detection of wormhole attacked nodes. The neighbour node ratio is simple ratio and it is measured with the help of two parameters; they are distance and communication range. Compared to the conventional methods which employed computationally expensive methods like digital signature and absolute time deviations, the proposed NNR-AODV has employed a very simple and effective method. Moreover, the proposed method showed its effectiveness in the detection of both external and internal wormhole nodes. In the simulation analysis, the effectiveness is proved by comparing its performance with several existing methods.

ACKNOWLEDGEMENT

Authors acknowledge the immense help received from the scholars whose articles are cited and included in references of this paper. The authors are obliged to authors/editors/publishers of all those articles, journals and books from where the literature of this paper has been reviewed.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive it.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	Conceptualization, software, methodology, validation, formal analysis, investigation, M V D S Krishna Murty; writing—original draft preparation, M V D S Krishna Murty; writing—review and editing, M V D S Krishna Murty, Lakshmi Rajamani

REFERENCES

1. G. A. Walikar, R. C. Biradar, A survey on hybrid routing mechanisms in mobile ad hoc networks, Journal of Network and Computer Applications77 (2017) 48-63. [CrossRef]
2. M. K. Gulati, K. Kumar, A review of qos routing protocols in MANETs,in: 2013 International Conference on Computer Communication andInformatics, 2013, pp. 1-6. [CrossRef]
3. M. M. Alani, Manet security: A survey, in: 2014 IEEE ICCSCE, 2014,pp. 559-564. [CrossRef]
4. M. Amadeo, C. Campolo, A. Molinaro, Forwarding strategies innamed data wireless ad hoc networks: Design and evaluation, Journal of Network and Computer Applications 50 (2015) 148-158.587. [CrossRef]
5. S. Kalita, B. Sharma, and U. Sharma, ``Attacks and countermeasures inmobile ad hoc network an analysis,'' *Int. J. Adv. Comput. Theory Eng.*,vol. 4, no. 3, pp. 16-21, 2015.
6. H. L. Nguyen and U. T. Nguyen, ``A study of different types of attackson multicast in mobile ad hoc networks,'' *Ad Hoc Netw.*, vol. 6, no. 1, pp. 32-46, 2008. [CrossRef]
7. V. Teotia, S. K. Dhurandher, I. Woungang, and M. S. Obaidat, ``Wormhole prevention using COTA mechanism in position based environment over MANETs,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7036_7040. [CrossRef]
8. P. Kaur, D. Kaur, and R. Mahajan, ``Simulation based comparative study of routing protocols under wormhole attack in manet,'' *Wireless Pers.Commun.*, vol. 96, no. 1, pp. 47_63, 2017. [CrossRef]
9. J. Padmanabhan and V. Manickavasagam, ``Scalable and distributed detection analysis on wormhole links in wireless sensor networks for networked systems,'' *IEEE Access*, vol. 6, pp. 1753_1763, 2018. [CrossRef]
10. S. Geetha and V. C. Patil, ``Graph-based energy supportive routing protocol to resist wormhole attack in mobile adhoc network,'' *Wireless Pers. Commun.*, vol. 97, no. 1, pp. 859_880, 2017. [CrossRef]
11. G. Kumar, M. K. Rai, and R. Saha, ``Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in Wireless Sensor Networks,'' *J. Netw. Comput. Appl.*,vol. 99, pp. 10_16, Dec. 2017. [CrossRef]
12. F. A. Khan, M. Imran, H. Abbas, and M. H. Durad, ``A detection and prevention system against collaborative attacks in mobile ad hoc networks,'' *Future Gener. Comput. Syst.*, vol. 68, pp. 416_427, Mar. 2017. [CrossRef]
13. M. Tahboush and M. Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)," in *IEEE Access*, vol. 9, pp. 11872-11883, 2021. [CrossRef]
14. H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap and K. H. Wandra, "Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET," *2016 10th International Conference on Sensing Technology (ICST)*, 2016, pp. 1-6. [CrossRef]
15. S. Tripathi, "Performance Analysis of AODV and DSR Routing Protocols of MANET under Wormhole Attack and a Suggested Trust Based Routing Algorithm for DSR," *2019 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*, 2019, pp. 1-5. [CrossRef]
16. M. Shukla and B. K. Joshi, "A Trust Based Approach to Mitigate Wormhole Attacks in Mobile Adhoc Networks," *2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)*, 2021, pp. 776-782. [CrossRef]
17. S. Majumder and D. Bhattacharyya, "Mitigating wormhole attack in MANET using absolute deviation statistical approach," *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 2018, pp. 317-320. [CrossRef]
18. S. N. Ghormare, S. Sorte and S. S. Dorle, "Detection and Prevention of Wormhole Attack in WiMAX Based Mobile Adhoc Network," *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2018, pp. 1097-1101. [CrossRef]
19. A. Bhawsar, Y. Pandey and U. Singh, "Detection and Prevention of Wormhole Attack using the Trust-based Routing System," *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 2020, pp. 809-814. [CrossRef]
20. N. Al-Bulushi, D. Al-Abri, M. Ould-Khaoua and A. Al-Maashri, "On the Impact of Static and Mobile Wormhole Attacks on the Performance of MANETs with AODV and OSLR Routing Protocols," *2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA)*, 2020, pp. 1064-1069. [CrossRef]
21. M. Prasad, S. Tripathi and K. Dahal, "Wormhole attack detection in ad hoc network using machine learning technique," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, pp. 1-7. [CrossRef]
22. S. Sharma and R. M. Sharma, "EPPN: Extended Prime Product Number based wormhole DETECTION scheme for MANETs," *2017 11th International Conference on Intelligent Systems and Control (ISCO)*, 2017, pp. 251-254. [CrossRef]
23. H. As'adi, A. Keshavarz-Haddad and A. Jamshidi, "A New Statistical Method for Wormhole Attack Detection in MANETs," *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, 2018, pp. 1-6. [CrossRef]
24. M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi and A. Mammeri, "Graph-based wormhole attack detection in mobile ad hoc networks (MANETs)," *2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ)*, 2018, pp. 1-6. [CrossRef]
25. K. N. Venkata Ratna Kumar, M. R, C. M. Rao, P. N. Rao and K. S. Rao, "Intrusive Detection of Wormhole Attack Using Cluster - Based Classification Model In MANET," *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2022, pp. 1869-1874. [CrossRef]
26. F. A. F. Alenezi, S. Song and B. -Y. Choi, "SWANS: SDN-based Wormhole Analysis using the Neighbor Similarity for a Mobile ad hoc network (MANET)," *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2021, pp. 653-657.
27. B. Bhushan and G. Sahoo, "Detection and defense mechanisms against wormhole attacks in wireless sensor networks," *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, 2017, pp. 1-5. [CrossRef]
28. Y. Sun and Y. Chen, "Detection of Wormhole Attacks in Wireless Sensor Networks Based on Anomaly Detection Algorithms," *2022 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE)*, 2022, pp. 777-782. [CrossRef]
29. R. Shukla, R. Jain and P. D. Vyavahare, "Combating against wormhole attack in trust and energy aware secure routing protocol (TESRP) in wireless sensor network," *2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE)*, 2017, pp. 555-561. [CrossRef]
30. K. D. Thilak, S. Saranya, K. Kalaiselvi, M. V. Anand and K. Kumaresan, "Secure Data Transmission in Wireless Adhoc Networks by Detecting Wormhole Attack," *2022 8th International Conference on Smart Structures and Systems (ICSSS)*, 2022, pp. 1-5. [CrossRef]

AUTHORS PROFILE

M V D S Krishna Murty, completed B.E. in CSE from University of Madaras, Chennai and M. Tech in CS from JNTU, Hyderabad. Currently, he is a research scholar in the department of CSE at JNTUH, Hyderabad. His area of interests are MANETs and Machine Learning. He has 21 years of teaching experience and 5.5 years of industrial experience as a software professional. He has presented technical papers in the area of MANETs and Data Science at international conferences held in India . Also, he has publications in reputed international journals.

Dr. Lakshmi Rajamani, obtained Ph.D (CSE) from Jadavpur University, Kolkata and worked as a Professor and Head in the department of CSE at OUCE, Osmania University, Hyderabad. Her area of interests are Neural Networks, Fuzzy Logic and Network Security. She has several papers published in reputed international journals. Also, she has presented technical papers in international conferences held in India and abroad.