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 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, decides whether a wormhole is present or not. Furthermore, NNR-AODV can detect both external and internal nodes that a wormhole has attacked. Additionally, NNR-AODV derived a Neighbour node Threshold value based on the cumulative distances between nodes present in the wormhole attack. For experimental validation, we conducted an extensive simulation, and performance was measured through the Number of bogus links, Detection rate, False positive Rate, Packet delivery ratio, and Packet loss ratio. The obtained results demonstrate superior performance in detecting wormhole attacks compared to existing methods.

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

I. INTRODUCTION

Over the past few years, rapid progress in the development of Mobile Ad Hoc Networks (MANETs) has enabled various wireless applications that can be employed in diverse areas, such as Entrainment, Education, Military, Emergency services and Collaborative computing [1]. Due to the special characteristics of MANETs, namely independent infrastructure and self-organising nodes, MANETs have become an ideal choice for information sharing and communication. Thus, the mobile nodes of a MANET can execute both routing and hosting functions. In the case of routing, they function as relay nodes, forwarding data from one node to its destination using standard protocols. However, the central issue in MANETs is their mobility, which introduces several severe constraints on network lifetime, quality of service and security [2-4]. Due to the nature of decentralisation and openness of MANETs, mobile nodes are not reliable for constraining 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 the attack, they range from passive eavesdropping to severe battery draining. There are additional attacks that aim to tamper with data and conduct traffic analysis through eavesdropping. In general, attackers primarily focus on the resources of mobile nodes, including bandwidth exhaustion, battery depletion, and data manipulation. 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 attempt to disrupt the original behaviour of the network. An example of this type of attack is the wormhole attack (WHA), in which a routing loop is established by creating a wormhole node. Next, the internal attacks mainly target compromising internal nodes. They distribute false data and try to disrupt the data flow. Sybil, grayhole, and blackhole attacks are the best examples of this kind of attack.

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 falsely 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 challenging to detect. However, Chen *et al.* [12] hold the view that the wormhole attack is a typical external attack. Moreover, the majority of works in the literature pay excessive attention to external wormholes but ignore internal wormholes, which are also common in MANETs.

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

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 organised as follows: Section II explores the literature survey on wormhole detection methods. Section III examines the details of the proposed NNR-AODV. Section IV presents the details of the simulation experiments, and the final section concludes the paper.

II. LITERATURE SURVEY

In this survey, we have explored various earlier methods primarily aimed at detecting 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 the packet delivery ratio and hop count-based Round Trip Time (RTT) for external WHA detection. For internal WHA detection, they suggested computing the communication range between consecutive nodes in the network. This approach didn't use any external middleware or hardware. Additionally, it reduced energy consumption and delay by avoiding WH loads in the network. They utilised the NS-2 Simulator for experimental validation, employing performance metrics such as 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 tunnelling time taken by the tunnel for analysing the WH behaviour. Then, a threshold is determined, and based on these two values, the node is classified as either WH or not. Furthermore, they applied a hash-chain and digital signature algorithm to mitigate 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 can detect WHA in very little time, as the original path takes more time than the fake tunnel. The computation of the time taken for delivery helped identify the 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 places the packet in a different location and then forwards it to another compromised node, which is located away from the tunnel. A. Bhawsar et al. [19] calculated trust in the AODV routing protocol for the detection and prevention of WHA. This approach suggested a multipath selection to find the best routing path. All available paths are tested for WHA, and finally, one path is selected that 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 Optimised Link State Routing (OLSR) and AODV, for the 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 a network with multiple WH tunnels. In the next phase, they characterised packet attributes and, based on that, selected features. Then, they performed data collection and aggregation from a large volume of data sets. In the final phase, they applied a machine learning algorithm for WHA detection.

S. Sharma and R. M. Sharma [22] proposed a hop count model-assisted routing protocol called the Extended Prime Product Number (EPPN) to find WHA in MANETs. They computed the hop count of an active path between the source and destination and integrated it into the AODV protocol. Based on the obtained hop account value, WHA is detected if it exceeds the received hop count. H. As'adi et 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 does not 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 a 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-of-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 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 requiring specific location information and without generating any coordination and communication overhead. Furthermore, the SWANS also reduced the false negatives and false positives resulting from 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 an 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 a single hop between nodes. Additionally, this approach has minimal overhead and does not require any special hardware for time synchronisation. R. Shukla et al.[29] proposed trust and energy-aware secure routing protocol (TESRP) to provide security against WHA. This approach is considered one of the best, but it was unable to identify WHA. Hence, the authors used TESRP with a sequence number for security provision in the network from WHA.

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

Adversary nodes are identified on both sides of communication and discarded from the network. They brought a bundle of Miss Fortune adversary nodes to avoid packet loss and ensure data transmission occurs after the nodes are separated from the 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 was attempted successfully and effectively between the source and destination.

III. PROPOSED APPROACH

3.1 Overview

NNR-AODV aims to detect wormhole attacks in MANETs. A conspiracy between two malicious nodes typically initiates wormhole attacks. The two nodes are located at the ends of the network, far apart, and their configuration information will not appear in the routing table; therefore, 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 neighbour. Therefore, the standard transmission of data is disrupted, and subsequently, the network performance is affected.

3.2. Neighbour Node Ratio (NNR)

Verifying the trustworthiness of all nodes in a network is a time-consuming and battery-intensive process. Since only a few nodes can be compromised by WHA, they needed to be identified. In general, the attacks raise the network connectivity, and hence there is an apparent rise in the number of neighbours. Hence, the number of neighbour nodes that have an impact on WHA is more than that of a node not in the WHA scope. Therefore, we have proposed a threshold used to compare the neighbour number of all nodes in the network to determine the suspected nodes that 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 identification of suspected nodes is done as follows: 1. Every node knows its neighbour nodes after their deployment in the network. 2. Then, each node calculates its NNR and the average NNR of all its neighbouring nodes. 3. The NNR is compared with NNR_T To determine whether the requirement of the detection process is necessary or not.

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

3.3 Wormhole Detection

At this phase, the 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 to the suspected node pair that is in direct communication with each other. The central theme of EWHA detection is comparing the differences in hop count between exclusive neighbours of target nodes.

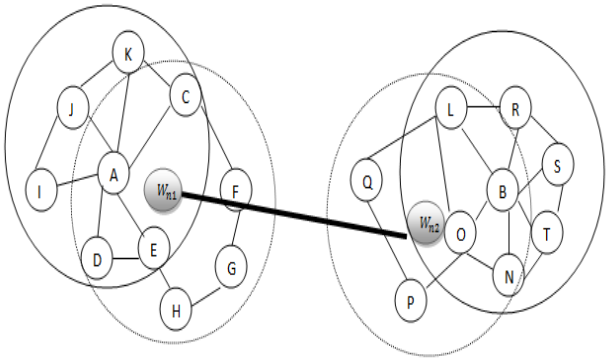

Figure 1: External Wormhole Attack

In Fig. 1, node A and node B assume that they are neighbours, and the nodes within the communication range mistakenly think that they are one-hop neighbours of each other. W_{n1}. Hence, the neighbour nodes of node A are denoted as $N_A = \{B, C, D, E, I, J, K, L, N, O, P, Q\}$. Similarly, the neighbour nodes of node B are denoted as $N_B = \{A, C, D, E, F, G, H, L, N, O, R, S, T\}$. Based on these two neighbour sets, the standard 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, the maximum hop count between any two nodes is one. However, based on this fact, it is seen that they are located much farther away from each other, and the original hop count is larger than 1.

Based on the above exploration, nodes can be chosen that have more than two exclusive neighbour numbers between any node pair, and new links are established among the set of exclusive neighbours. These must bypass the node of the other neighbour. 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 nodes A and B, then mention that any of the node links in the exclusive neighbour set $\{I, J, K, P, Q\}$The number 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 nodes A and B have an EWH between

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

them. Upon exceeding the hop count from the WH threshold, i.e., the link from node I to node P, nodes A and B discard the link from their routing tables and propagate the removed neighbour node 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, it is found that the links associated with WHs are significantly fewer than the WH threshold, and they are successfully detected and discarded from the network. However, some EWHs and IWHs exist, and their links are shorter, which are not identified during EWHA detection. Hence, IWHA detection takes that responsibility. According to the discussion above, the IWHA detection must be executed on the remaining nodes that have common neighbour nodes in the suspected node list. The central theme of IWHA detection is to activate node pairs in the suspected list that have common neighbours as proof to determine whether the data packets between them are forwarded or not. Initially, the pair of nodes that are ready for IWHA detection must undergo the current verification, where their neighbour nodes are unable to forward data at the time of verification, thereby preventing the issue. 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 determines that it has received irrelevant information, then the packets are resent from the sender node.

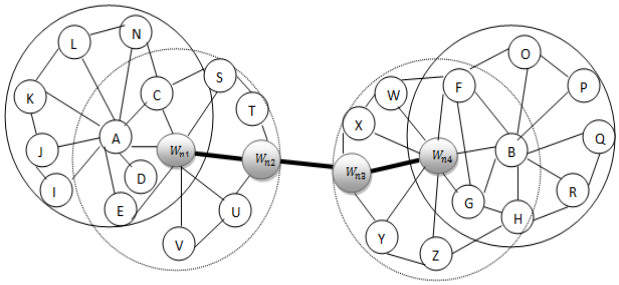

Figure 2: Internal Wormhole attack

As shown in Fig.2, a wrong assumption is made at nodes A and B about their one-hop 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 the link between node A and node B, the standard neighbour set needs to be determined as $N_A \cap N_B = \{C, D, E, F, G, H\}$. This set is used as evidence for local monitoring. Until they obtain the right of verification, the common neighbours of nodes A and B are unable to send messages. The standard node set, i.e., $N_A \cap N_B$Node A then moves into the monitoring state. Then, node A formulates an authentication packet mentioning the destination's address and sends it to node B. After the packet transmission, node A and the evidence nodes can hear three possible types of packets. They are -1) Node A's forwarded packet, 2) Node B's reply packet, and 3) other nodes' 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 $A \rightarrow B$ is 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 an overhearing about the forwarding of an 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 $A \rightarrow B$ is 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. Suppose the reply sent by node B is received at node A within the specified time (denoting the maximum possible communication delay in MANETs). In that case, node A assumes that the WH is not present between node A and B, regardless of the value of s. During the monitoring phase, if node A finds that the packet has been forwarded, it assumes that the WH is present between node A and B, regardless of the value of s. 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 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, nodes A and B discard each other from their monitoring tables and then propagate the updated information to their different 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 B is equal to the communication radius. Under these conditions, the path hop count increases to 4.

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)

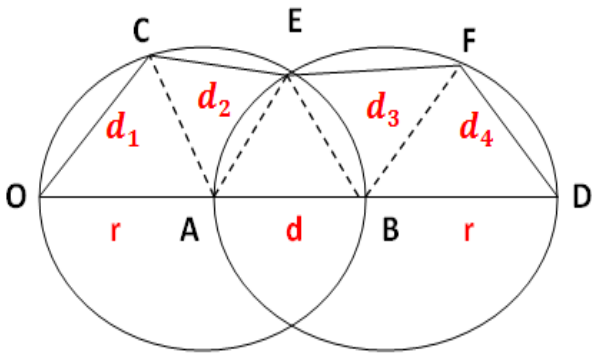

Figure 3: Node Communication Model

As shown in Fig. 3, it is observed that if a WH exists 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' If the value is less than the WH threshold, then it is declared that there is no WHA; otherwise, nodes A and B assume that they are likely to be attacked by WHA. However, such a strict declaration may succeed only in some instances. For example, some nodes on the path may have very little residual energy and hence can't cooperate. In such conditions, decisions based on just hop count result in larger false positives. Hence, to reduce such errors, paths with more hop count than the WH threshold are kept under testing. For such paths, an additional path trust evaluation is performed.

IV. SIMULATION ANALYSIS

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

4.1 Simulation Setup

Under the simulation setup, an initially random network is created with N nodes, and the network area is considered to be 1000 m × 1000 m. The creation of the simulation setup is done in such a way that the random nature of the mobile node can be realised. This means that for every simulation, the node positions change randomly, thereby causing the neighbouring nodes also to change. Once the mobile nodes are deployed in the network, each node identifies its neighbour nodes based on their communication range. After the discovery, the source node broadcasts a route request packet, and based on the route replies received, a final path is established. Then, data transmission starts to the destination node. After the completion of data transmission from source to destination, the performance is analyzed through several performance metrics. To analyse the performance of the proposed approach, various simulations are conducted by varying different network parameters. Table 1 shows the simulation setup 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 the Length of the 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: the number of bogus links, the Malicious Detection Rate (MDR), and the False Positive Rate (FPR). They are measured using varying node parameters, such as Node Degree, Wormhole Number, and Neighbour Node Ratio Threshold.

Node Degree: The degree of a node is the number of edges connected to the node, which can also be considered the average number of nodes within a node's communication range. Eq.(4.2) shows the calculation of *Node Degree*, where r_{max} The maximum transmission range of nodes, N, represents the total number of nodes. L and W denote the length and width of the network area, respectively. When N = 40, the Node Degree is 12, i.e., there are approximately 12 nodes within 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 the proposed method is analysed through five performance metrics: 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 the number of wormholes, node degree, and node count. The results obtained are illustrated in the figures that follow.

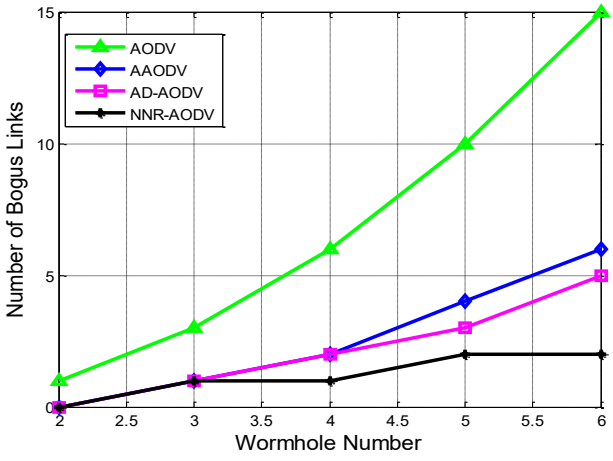

Figure 4: Number of bogus links for varying wormhole count

Fig. 4 shows the impact of wormhole count on the creation of the 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 indicate that AODV exhibits a linear increase in the number of bogus links with an increase in the wormhole count. Compared to the traditional AODV, the remaining methods involve a wormhole prevention mechanism and hence experience a smaller number of bogus links than AODV. For instance, at a wormhole node count of 4, the number of bogus links for AODV is observed to be 6, whereas for AD-AODV, AAODV, and NNR-AODV, it is 2, 2, and 1, respectively. On average, the number of bogus links for AODV is observed to be 8, while for AD-AODV, AAODV, and NNR-AODV, it is observed to be 3, 2, and 1, respectively.

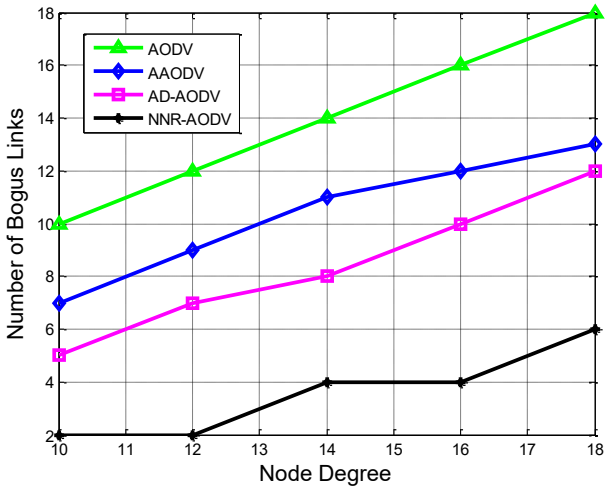

Figure 5: Number of bogus links for varying node degree

Fig. 5 illustrates the effect of node degree on the creation 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 the network length to 18%. For a wormhole node, the larger node degree reveals the greater number of neighbour nodes. As the number of neighbour nodes increases, the wormhole node attempts to create more bogus links with them, and consequently, the number of bogus links increases with an increase in node degree. The results shown in Figures 4 and 5 demonstrate the increasing characteristics of bogus links with the node degree for all methods. However, the proposed NNR-AODV has experienced a slower increment compared to conventional methods, as it adapts a neighbour node ratio, which is an essential aspect of wormhole attacks. Thus, NNR-AODV has a lower number of bogus links. Among the methods, AODV has experienced a higher number of bogus links, as it lacks a mechanism to prevent wormhole attacks. On average, the number of bogus links for AODV is observed to be 14, while for AD-AODV, AAODV, and NNR-AODV, it is observed to be 10, 8, and 3, respectively. Conventional methods are ineffective in detecting external wormhole nodes or 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 in AODV sometimes increases rapidly and sometimes slowly because the nodes are deployed randomly, and newly deployed nodes may not be within the communication range of the wormhole node.

Fig. 6 shows the impact of wormhole number on the detection rate. Additionally, the detection rate decreases with an increase in the number of wormholes. With the rise in wormhole nodes, nodes can establish a greater number of bogus links, and detecting all such links is a typical issue. Hence, the number of bogus links detected is lower, resulting in a lower detection rate. Even though the detection rate is decreasing, the proposed approach maintains an effective detection rate at all instances of wormhole count. Since the proposed mechanism applies a neighbour node ratio, a fundamental feature of wormhole attacks, it can identify wormhole nodes even in multiple instances. Hence, it achieved a better Detection rate compared to existing methods.

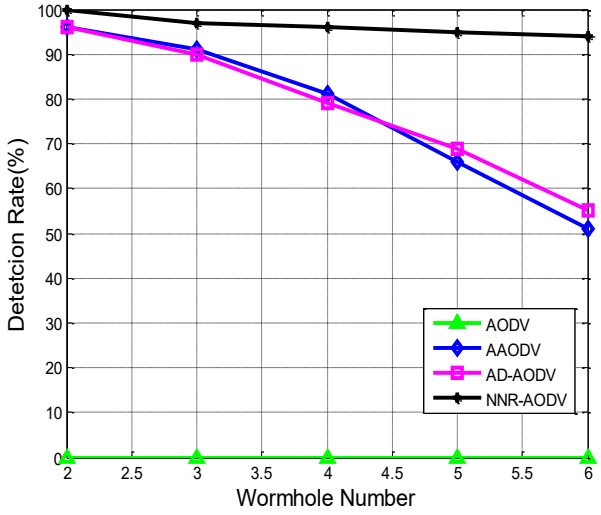

Figure 6: Detection rate for varying wormhole count

The existing methods have shown a rapid decline in detection rates, accompanied by an increase in wormhole counts. AAODV employed digital signatures to prevent wormhole attacks and used the tunnelling time taken by the tunnel to analyse the behaviour of wormholes. For the distant wormhole node pair or normal node pair, the tunnelling time is significant, and in such a condition, identification is challenging. Next, AD-AODV applied absolute deviation in time for the identification of wormhole nodes. Compared to the neighbour node ratio, the time-based measures are less significant and contribute less to wormhole node detection. Hence, the proposed approach achieved a higher detection rate than the conventional methods. On average, there is no detection rate for AODV, while for AD-AODV, AAODV, and NNR-AODV, it is observed to be 77.2532%, 78.4230%, and 96.4215%, respectively. FPR follows an inverse relation with the detection rate; hence, the results shown in Fig. 7 are increasing in nature with an increase in wormhole number.

Generally, a false positive is defined as a node that is declared as a wormhole node but, in reality, it is not; i.e., the node is mistakenly identified as a wormhole node. The accumulation of such false positives is used to calculate the FPR. As the number of wormhole nodes increases, the FPR also increases, as the detention methods aim to identify all wormhole nodes effectively.

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)

However, the proposed method achieves a better FPR than conventional methods, as it employs a simple and effective NNR mechanism for identification. As AODV has no detection mechanism, it has experienced the maximum FPR. Next, the average FPR of the proposed NNR-AODV is observed to be 7.2222%, while for AD-AODV and AAODV, it is observed to be 23.63232% and 26.4578%, respectively.

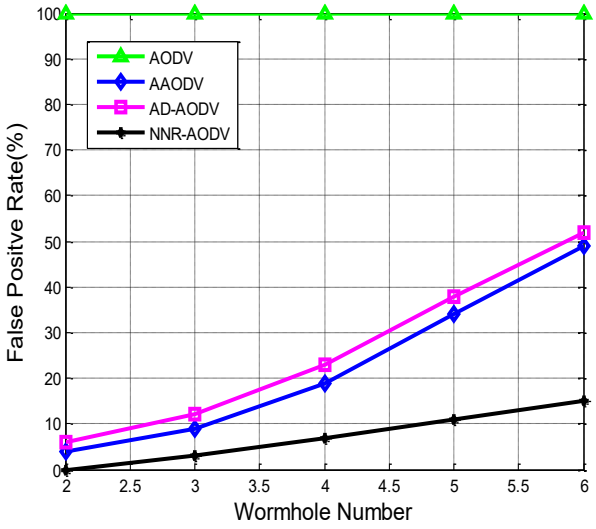

Figure 7: False Positive Rate for varying wormhole count

Upon the occurrence of a 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 the destination. In this process, upon receiving the data, the wormhole nodes may or may not forward the data to the destination, or may send only partial data. In both cases, the source node loses some packets, resulting in lower PDR at the destination node. In the case of a larger node count in the network, the number of bogus links is significantly higher, and it stops sending data to destination nodes effectively. Due to these reasons, the PDR decreases and the PLR increases as the node count in the network increases. However, the proposed approach is practical in identifying wormhole nodes in the network, which can help nodes achieve effective data transmission between source and destination nodes. Hence, the proposed method achieved a higher PDR and lower PLR, even for a larger number of nodes in the network. From Fig. 8, the average PDR of NNR-AODV is observed to be 80.2315%, while for conventional methods, it is observed to be 62.4512%, 57.5555%, and 34.7520%, respectively, for AD-AODV, AAODV, and AODV. Next, from Fig. 9, the PLR for the proposed approach is observed to be lower, with an approximate average value of 20.3323%. In contrast, for conventional methods, the observed percentages are 37.2512%, 42.5277%, and 65.3014% for AD-AODV, AAODV, and AODV, respectively.

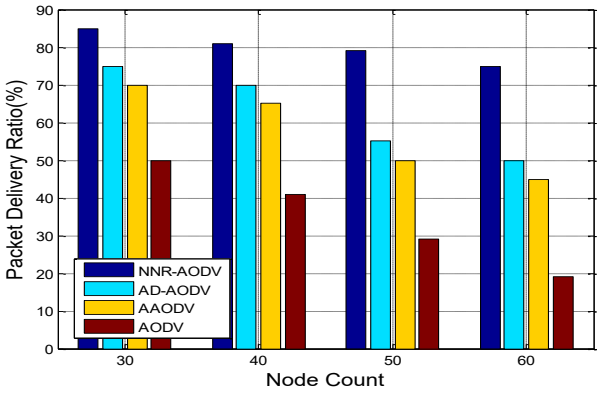

Figure 8: Packet Delivery Ratio for varying node count

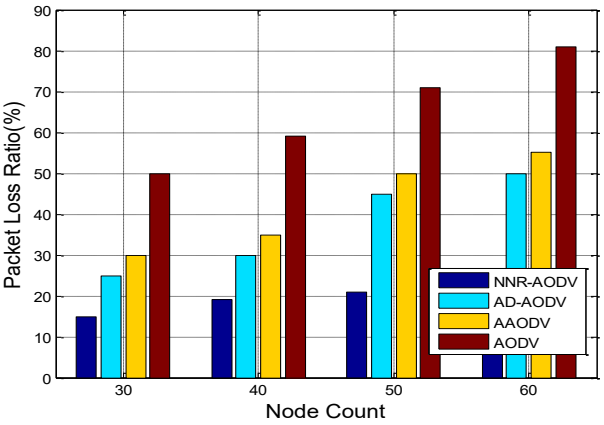

Figure 9: Packet Loss Ratio for varying node count

VI. CONCLUSION

In this paper, we discuss a new method proposed for detecting wormhole attacks in MANETs. The proposed NNR-AODV is lightweight and straightforward, thereby preventing nodes in MANETs from being vulnerable to wormhole attacks. NNR-AODV utilised a simple neighbour node calculation for the analysis and detection of wormhole-attacked nodes. The neighbour node ratio is simple and is measured using two parameters: distance and communication range. Compared to conventional methods that employ computationally expensive methods like digital signatures and absolute time deviations, the proposed NNR-AODV uses a practical and straightforward approach. Moreover, the proposed method demonstrated its effectiveness in detecting both external and internal wormhole nodes. In the simulation analysis, the effectiveness is shown by comparing its performance with that of several existing methods.

ACKNOWLEDGEMENT

The authors acknowledge the immense help received from the scholars whose articles are cited and included in the references of this paper. The authors are obliged to the 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 or consent to participate, as it presents evidence that is not subject to interpretation.
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 Applications 77 (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 and Informatics, 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 in named 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 in mobile 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 attacks on 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 ad hoc 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 localisation 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 Neighbour 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 defence 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 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 the University of Madras, Chennai and M. Tech in CS from JNTU, Hyderabad. Currently, he is a research scholar in the Department of CSE at JNTUH, Hyderabad. His areas of interest 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 areas of MANETs and Data Science at international conferences held in India. Additionally, he has published in reputable international journals.

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