A Wormhole Attack Detection and Prevention Technique in Wireless Sensor Networks

Marcus Okunlola Johnson
Computer Science & Informatics
University of East London (UEL)
London, UK

Arish Siddiqui
Computer Science & Informatics
University of East London (UEL)
London, UK

Amin Karami
Computer Science & Informatics
University of East London (UEL)
London, UK

ABSTRACT

Security is one of the major and important issues surrounding network sensors because of its inherent liabilities, i.e. physical size. Since network sensors have no routers, all nodes involved in the network must share the same routing protocol to assist each other for the transmission of packets. Also, its unguided nature in dynamic topology makes it vulnerable to all kinds of security attack, thereby posing a degree of security challenges. Wormhole is a prominent example of attacks that poses the greatest threat because of its difficulty in detecting and preventing. In this paper, we proposed a wormhole attach detection and prevention mechanism incorporated AODV routing protocol, using neighbour discovery and path verification mechanism. As compared to some pre-existing methods, the proposed approach is effective and promising based on applied performance metrics.

Keywords

Wireless Sensor Networks, Wormhole Attack, AODV routing

1. INTRODUCTION

A Wireless sensor network is a collection, and grouped specialized of transducer embedded with a communication infrastructure capabilities, for the monitoring and keeping records of conditions at different locations [3]. Such as temperature, pressure, speed of wind direction and more importantly, vital human body functions. A sensor network should contain an autonomous node where every node is interconnected to sensors, with communication range, an amount of power and bandwidth. There are four basic parts that makes up a network sensor; sensing units, a processor, a transceiver, and a battery [10]. Electrical signal in the transducer is generated based on the physical quantity. While a microcomputer processes and store this sensor output. Furthermore, to the processing, the transceiver receives commands from a central computer for onward data transmission. All this process is powered up by a battery.

Wireless sensor network unlike wired networks, contains spatially distributed nodes in an unguided and unattended environment, hence the possibilities of an attack by adversary is highly likely [2]. Therefore, the need to keep this sensor nodes save from attack is enormous. For a sensor network nodes, to be able to send packets and communicate between them, partnership between nodes has to be established, because a single node transmission range is limited and cannot transmit packets to a long distance. This process by which a node determines its neighbour is called a neighbour discovery. Once communication is established between nodes, a link is then formed to transmit the packet in a single hop distance. This process is repeated until packets arrived at its destination. It is during this routing process that an adversary can attack the network with malicious nodes acting like a real neighbour to the source and destination nodes. Ones malicious node is able to attached itself to a genuine node, it creates a low latency link between the malicious nodes, for a falsely packets transmission. One of many of such attacks that causes huge impact on the network sensor is called wormhole attack. One of the reason for this attack is to disrupt the neighbour discovery mechanism [18]. Hence, the security assessment in this process, is paramount to the overall security enhancements of neighbour discovery protocol.

Designing an accurate attack detection mechanism alongside with a prevention technique in network and communication infrastructures are highly challenging and ongoing research work, attracting a wide range of researchers' attention [15, 16, 17]. In this research work, evaluation is concentrated on wormhole attack; an attack that causes disruption in a network setup by confusing routing mechanism, giving an illusion that genuine sensor nodes are neighbours to a malicious node. This research aims to detect and prevent this attack in the routing protocol AODV using NS2 network simulator. Since data analytics are some of the most effective defences against network attacks [13, 14], we will analyse this attack node from an attacker's perspective using an existing algorithm and suggest new improvement on the existing detection for the continued functionality. The rest of the paper is organized as follows. Section 2 presents the wormhole implementation modes. Section 3 provides literature review. Section 4 details the proposed method. The experimental setup and results are desribed in Section 5. Finally, Section 6 draws conclusion.

2. WORMHOLE IMPLEMENTATION MODES

Wormhole attacks occurs at the network layer of OSI model, and it is classified into four attacks modes [5] as follows:

(1) *Encapsulation*: It is a type of wormhole attack where a malicious node at one part of the network overhears the RREQ packet. It is then tunnel through a low latency link with the help of normal node, to the second colluding malicious node at a distance near to the destination node. Once this packet is received by the second malicious code, the legitimate neighbour of the node drops any further legitimate requests from a

legitimate neighbour node. This result to the routes between the source and the destination go through the wormhole link, because it has broadcast itself has the fastest route. It prevents legitimate nodes from discovering legitimate paths more than two hops away.

For example, in Figure 1 where A and B finds the shortest path between them for packet transmission, where two malicious nodes X and Y is present. Node A will broadcast a RREQ but because a wormhole node is present X gets this route request and encapsulates it into the packets destined for Y, and it transmit this packet through a wormhole link tunnel. When this packet is received by Y, it unmarshals the packet and rebroadcast. B being the nearest neighbour to Y will receive this packet thinking it has come from a legitimate path. Due to the encapsulation, the hop count will not increase during the traversal through U-V-W-Z. Now Node B has two routes to choose from, either A-C-D-E or A-X-Y. obeying the rules of routing protocols that uses metric of shortest path to choose a route path. B will choose the shortest route path which happens to be a wormhole link. which is about 4 hops. And apparently, the wormhole link is 3 hops away while in reality is about 7 hops away.

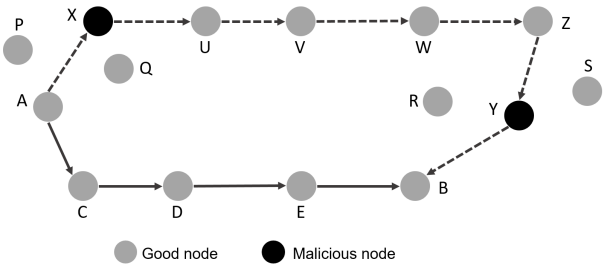


Fig. 1: Encapsulation Wormhole

(2) *Packet Relay*: This is another type of wormhole attack where malicious relays packet between source and destination nodes. Unlike encapsulation, this type of wormhole attack can be launched using only one malicious node. Considering node, A and B are two non-neighbours. With a malicious node X, it can replay packets between A and B giving the illusion that they are neighbours.

(3) *Out-of-band Channel*: As the name suggest is a type of wormhole attack that uses a long range directional wireless link or a wired link. It is a very difficult attack to launch because its needs a specialized hardware. For example, in Figure 2 malicious node X tunnels the route request to a legitimate node Y, a neighbour of B. Node Y broadcast the packet to its neighbour, which always happens to be the destination node. Node B gets two RREQ as A-X-Y-B and A-C-D-E-F-B. obeying the rule of most routing protocol, node B will choose the fastest and shorter route which happens to be the wormhole link.

(4) *High Power Transmission*: In this mode of attack, a single malicious node can create a wormhole without colluding node. when this single malicious node received a RREQ, it rebroadcasts the request at a very high power level capability compared to normal node, thereby attracting normal nodes to overhear this RREQ and further on broadcast the packet towards destination.

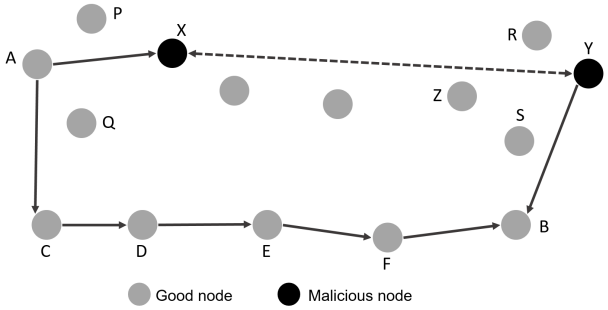


Fig. 2: Out-of-Band Wormhole

3. LITERATURE REVIEW

Wireless sensor nodes are prone to different types of attacks, because of its spontaneous nature in an unprotected environment where several security threats exist. Some of these attacks can include wormhole attack which can cause denial of service. Up till date various techniques has been proposed for the detection and prevention of wormhole wireless sensor node attack. The application of most of the proposed solutions is promising, but the possibility of malicious nodes affecting the good ones, coupled with the difficulty in distinguishing the relationship between a poor network and affected nodes behaviour must be addressed.

3.1 Reactive Protocols

A brief explanation to the most important reactive protocols (AODV and DSR), is simulated in NS-2 [10] and Qualnet simulator [1]. Both simulators conclude wormhole disrupts the three performance of routing protocol namely, throughput, end to end delay and packet delivery ratio under wormhole attack. Gaurav Garg [9] discussed AODV is more vulnerable to wormhole attack in mobility state while DSR is least vulnerable in non mobility state.

3.2 Neighbour Discovery Approach

Wormhole attacks is one of the most powerful WSN attack that does not require any cryptographic breaks, as this attack does not create a separate packet. Its impact in the network and types is well described in-depth, alongside detail analysis on the detection and prevention techniques. Result obtained indicates when a packet is received, sent or dropped at the nodes due to attacks, an explanation of how the network is affected in terms of throughput variations is well analysed [25]. In the same sense, a detail review is discussed and simulated using NS-2 on the prevention of wormhole attack in mobile Ad Hoc network using neighbour node analysis. Details relating to the neighbouring nodes is analysed to check the authenticity of the nodes. In this approach, a node can request information stored by its neighbouring nodes in order to carry out a route request (RREQ) and a route response (RREP) mechanism.

Sun Choi [7] proposed a simple scheme named WAP (Wormhole Attack Prevention) algorithm to prevent wormhole attack. WAP which operates on DSR protocol where generally, each node does not check a RREQ packet overheard from its neighbour nodes. In this scheme, all nodes monitor their neighbour?s behaviour when a route is requested by using neighbours list. This mechanism also uses wormhole prevention timer, because it is difficult to use only neighbour monitoring to detect wormhole attack as malicious node acts like a legitimate neighbour. For this reason, WPT calculates time delay per hop in the route and it records the neighbour?s nodes

address and time of receiving the packet. When a node overhears a route request after wormhole prevention timer, then a wormhole attack is taking place. If a wormhole link is found, the information is stored at the source node to isolate them from taking part in the routing again. This is effective because it does not stop the flow of packets between legitimate nodes. However, it suffers from false positive. WADP is an improved WAP by Juni Biswas [4] for wormhole attack detection. It combines node authentication to remove false positives and helps in exact location mapping of wormhole in a modified AODV routing protocol.

3.3 Digital Signature Approach

In defending against malicious nodes using digital signature, this reasearch proposed a mechanism whereby verification of neighbours node signature is significant. In every legitimate nodes in the network there contains the digital signature of all the remaining legitimate nodes of the same network. For example for a route request to take place, sender first create a secure route between source and destination. This in turn distinguish between legitimate and malicious nodes, because malicious nodes does not possess the original digital signature [22].

In the same sense Amarijit et al. [20] developed a novel technique combining both princicles of clustering and digital signature during route discovery using the same AODV routing protocol. Information of all nodes is grouped in different clusters, and each cluster has a cluster head and a gateway nodes which forms a communication link to different cluster head in the same network. To establish a route betweeen nodes, it must first send route request to its cluster head. This cluster head will further forward the request to the other clusters after it has been digitally signed using a private key contained in the cluster head; through the gateway link until the request reaches the cluster head of the cluster which belongs to the destination node. Simulation result for this research prooved it archieved high level of detecting and preventing wormhole attack.

Transmitting data in a network efficiently is the key most important aspect of routing. Marti et al. [21] proposed two techniques watchdog and pathrater in detecting malicious node with minimal effect on throughput in the presence of misbehaving nodes. One of this technique is called watchdog. It is used for every nodes in the same network to detect any misbehaving node. When a packet is sent to the next hop, it tries overhear the packet forwarded by the next hop. For example a path from S to D through nodes A,B and C. node A cannot transmit to C without an intermediate node B. therefore when A transmits to B for onward forward to C, A will often tell if B transmit the same packet successfully to the correct node C otherwise it considers the next hop as malicious node. The pathrater uses the information about misbehaving nodes gained from the first technique (watchdog) to pick the route which is most likely legitimate. Every node maintains a trust rating for each of the nodes in the network. When watchdog detects a malicious node, the trust rating of the node is updated negatively. Techinically the pararater calculates a path metric by averaging the nodes ratings in the path to pick a safe route to send packets. This solution however, is better suited for traditional networks based on emphasis on the reliability of point to point communication than to sensor networks.

3.4 Local Monitoring Approach

Issa Khalil et al. (2005) [18] proposed two algorithms called MOBIWORP in the elimination of any wormhole attack when ad-hoc is in a mobility state. In this research paper a node is assigned to be the central authority which monitors the nodes neighbours locally. If any malicious nodes is found, it isolates the node globally. The proposed algorithm uses local monitoring of all neighbouring nodes and relies on a secure central authority for positiontracking of the mobile nodes. The use of central authurity is contacted only in the event of motion. Central authority node will still operate through periods in the event that its unreachable. The first proposed algorithm is selfish move protocol (SMP). In this protocol, the mobile node can only generate, send and receive its own traffic. This design arises from the knowledge that a node can only be able to launch an attack by forwarding packets. However, this protocol may cause a disconnection in the network if a large part of the nodes moves at the same time. To address this issue, the researcher developed a second algorithm called connectivity aided protocol with constant velocity (CAPCV). This protocol eliminates lack of connectivity thereby allowing the mobile node to forward packets.

3.5 Special Hardware-based Approach

Generally, the most common method to detect and prevent wormhole is the use of neighbour discovery mechanism. Sometimes they are achieved through the use of special hardware such as directional antennal [11]. Similarly, Srdjan Capkun [6] proposed SECTOR based on a special hardware. Others approaches towards this attack includes time synchronization for detection of whether packets sent from an authorized neighbour are received on time by the legitimate node [8]. Hu et al. (2003) [12] Introduced packet leashes in defending against wormhole attack. Two solutions were introduced, temporal and geographical. With geographical leashes, location information from GPS devices which is included in the packets, is used to detect the presence of wormhole nodes. And with temporal leashes, nodes are tightly time synchronised, thus packet transmitted between source and destination contains time at which it was sent. Furthermore protocols can be adjusted to estimate the distance betweeen the sender and the receiver. Using the network signal, it can be verified whether or not the data comes from the node within the range of communication.

3.6 Statistical Analysis Approach

Some other approach in this regards applies a centralised mechanism that makes use of statistical analysis for the detection of malicious node [23]. This mechanism can detect the presence of a malicious node due to specific changes in the statistical pattern. Analysing the issue of encrypting and decrypting packets sent across each node. Pravin Khandare et al. [19] used the RSA technique for encryption and decryption of the nodes. It uses the 2Ack mechanism to check that only the authenticated node receives the data. Acknowledgement is taken from one hop and two hop nodes. In cases where an attacker tries to forward the received message into another location, this mechanism will prevent this by taking the acknowledgements from the next two nodes.

3.7 Routing Protocol

To discover multiple paths between the source and the destination, we applied a reactive routing protocol called Ad hoc On-Demand Distance Vector (AODV) which was developed on July 2003. AODV offers quick adaptation to dynamic link conditions and uses low processing and memory overhead between participating mobile nodes in an established network. AODV routing table fields consist of *destination IP address*, *sequence number of destination node*, *hop count to destination* and *next hop to follow*. It also defines three types of control messages for up to date route maintenance [24]:

—RREQ: every route request carries a time to live (TTL) value that indicates the number of hops the packet should be forwarded. It is set to a predefine value at discovery stage and increased at retransmission if no reply is received by the receiving node.

—RREP: Route reply message is rebroadcast back to the source of a RREQ to confirm if the receiver is the real request address user or a valid route to the requested address.

—RERR: All node monitors the activities and link status of their neighbour in active route path. When there is a breakage in the link, a RERR message is broadcasted to notify other nodes of the lost link. For this to be activated, each node has to keep information such as IP address for each of its neighbours.

In On-demand distance vector routing protocol, each node maintains a routing table and gets updated every time a routing message is received. For a source node to send a packet, it broadcast Route request message to the whole of the network. On acknowledging the request by the other nodes, it checks if the corresponding route exist and check to make sure is not a repeated request. If it is a repeated one, the node simply discard the packet. If not the request will be accepted. This process is repeated till packets gets to its destination. The intermediate node to the destination node will send a route reply RREP to the source of the packet using a reverse route.

4. THE PROPOSED METHOD

There are two important parts contained in the detection and prevention of wormhole attack, neighbour and path verification. Two fake node neighbours with a wormhole tunnel will generally not share a common one hop neighbour node. while two genuine node neighbours will generally share other true neighbours between them. The proposed technique is to improve the existing algorithm in [26]. This technique will detect wormhole and isolate them from the route path. During the neighbour route discovery, the packet will be encrypted at each level by sharing *hello messaging* with neighbouring node. The packet will be decrypted by the receiving node and message must matched with the one distributed.

4.1 Algorithm Description

This work is based on the prevention of wormhole attack in a particular network. In this research, a detection and prevention mechanism is proposed in securing the communications between source and destination node. When sensor node wants to start communication, the first thing it does is a neighbour discovery from the neighbour list. It generates an encrypted beacon message with a secret key. As soon as the neighbouring node receives this beacon frame, it will be decrypted and the acknowledgement (RREP) is sent back to the sender.

4.1.1 Neighbour verification. The following steps will verify a neighbouring node in the network.

Building one-hop transmission neighbourhood list: Two neighbour nodes such as S and P which has their neighbour has $N_{(S)}$ and $N_{(P)}$ individually. Their neighbour list information exchange will be shared through a beacon messages. E.g. node S notifies its nearest neighbour $N_{(S)}$ with a periodic beacon message.

Building two-hop transmission neighbourhood list: Each node will request its neighbours to collect information about their neighbours list by way of transmitting beacon messages to its neighbours. This will enable each node to hold two hop information about their neighbours. For example, information exchanged between nodes A, B and C. Node(A) sends a beacon message to its neighbour Node(B), after this message is sent, the transmission range of Node(A) is increased to $2r$. After this increase, node(A) broadcast beacon message containing node(B) information to its neighbour of node(C). during this message, both nodes B and C will not change their transmission range. After node(C) hears this broadcast, it then verifies the authenticity of node(A) from node(B) because both node A and B had earlier exchange their information in the first broadcast. The beacon frame will be transmitted at regular intervals until packet gets to its destination successfully. After each change in radius of transmitting nodes, a test nodes updates its neighbour node in the next beacon time.

—If $N_{(C)}$ contains $N_{(B)}$ but not contained in $N_{(A)}$ then wormhole detected

—If $N_{(C)}$ contains $N_{(B)}$ and meets $N_{(A)}$ then no wormhole is detected

The schematic of the proposed algorithm for wormhole attack detection and elimination is given in Figure 3.

4.1.2 TRM AODV: Wormhole Attack Detection. **Input**: Wormhole path for data transmission, neighbours information. **Output**: Wormhole detection, periodically update the neighbour list using beacon.

The node A and B is used as two tested nodes to describe the main wormhole detection procedure of TRM algorithm. In proposed algorithm, all nodes in the network has a current information of its neighbours. Moreover, the neighbour list is updated frequently. Each node will request its neighbours to retrieve their neighbour lists by sending a beacon message to its neighbours. At the discovery stage, all nodes will send its own neighbour information to its neighbours by sending beacon frames. Using this steps, each node can get its neighbour details within two hops. At the end, network topology will be founded. The beacon information will be sent at regularly at intervals. After changing the radius transmission range, a test node will update its neighbour node details in the next beacon time. By comparing its current neighbour details with the previous details, a test node can now establish the existence of false topology if any, that should not exist in a normal network.

4.1.3 APS AODV: Wormhole Free Alternate Path Selection (The proposed method). **Input**: Wormhole attack detection. **Output**: Secure data transmission via attack elimination.

After wormhole detection, if wormhole link exists in that current route, then block that route and update it in the routing table. Another route is fetched from the routing table for secure data transmission. Hop count of alternate path is compared with the current path. Hop count will be higher in alternate path than wormhole path. In such case, alternate path is confirmed with the availability of alternate path without the involvement of wormhole nodes. Algorithm 1 provides the pseudocode of the proposed APS AODV (Alternative Path Selection by AODV) algorithm for wormhwhole attack detection and elimination.

5. EXPERIMENTAL RESULTS

The performance of the base paper TRM AODV is evaluated for the simulation settings as per the following model and compared with the proposed proposal (APS AODV) and also with normal scenario in which there is no wormhole present. In addition, to assess the robustness and effectiveness of the proposed method, we compare the results with a pre-existing algorithm developed in [2] called AOMDV. We conducted experiments on Network Simulator 2.35 (NS-2) which is an open-source discrete event simulator in the research of computer communication networks. NS2 consists of

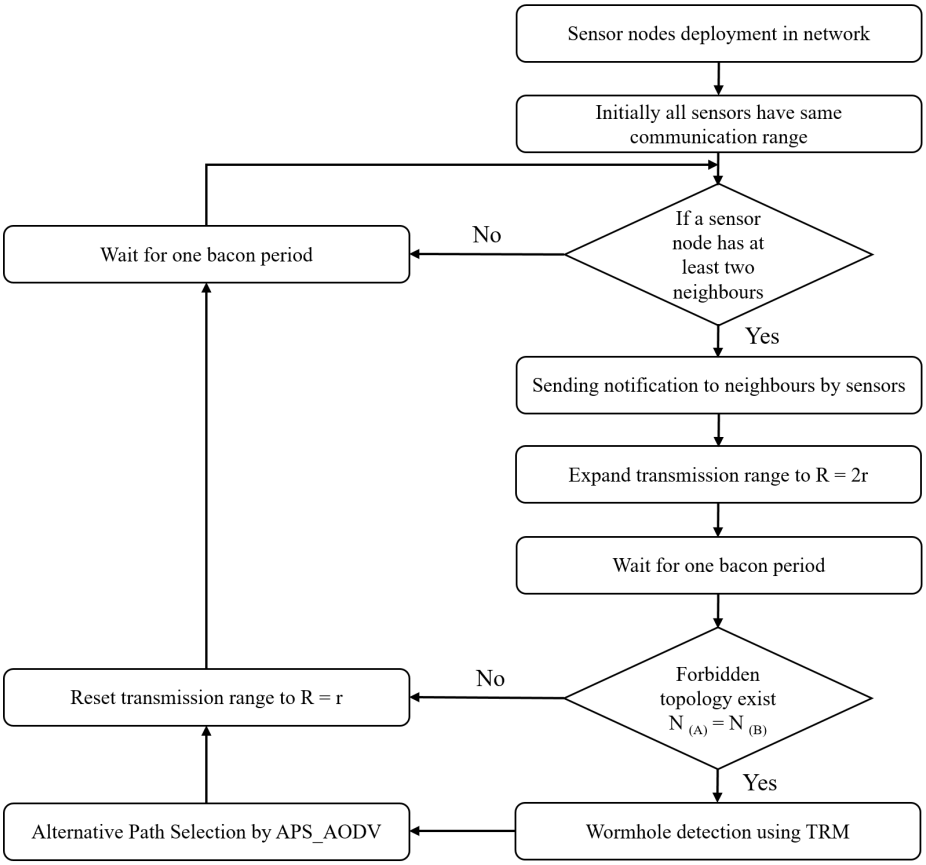


Fig. 3: The flowchart of proposed algorithm

Data: Given: Network N with node radius r, nodes n and m are nearest neighbours, wormhole number c = 0
Result: wormhole detection and elimination
Starts RREQ;
Generate HELLO beacon message while all sensors maintains the same communication range;
while *check every node in N* **do**
  expand radius of m to R = 2r;
  for *each node n in* $N(m)$ *do* **do**
    if *there exists once* $d \in N_n$ *and* $d \notin N_m$ **then**
      c = c + 1;
    else
      when wormhole link exists, fetch another route (verified by hop count comparison);
    end
  end
end

Algorithm 1: The pseudocode of the proposed method

two languages, C++ for internal mechanism (backend) of the simulation objects and OTcl for assembling and configuring the objects by schedluing the events.

5.1 Performance Metrics

The results obtained from four techniques are compared through three parameters including throughput (Eq. 1), end-to-end delay (Eq. 2), and packet delivery ratio (Eq. 3).

(1) **Throughput**: The amount of data successfully reached at the destination per unit of time.

$$Throughput\ (bits/s) = \frac{Total\ number\ of\ received\ pckts\ at\ dst}{Simulation\ time} \tag{1}$$

(2) **End-to-End delay**: The time taken for a packet to reach the destination from the source node.

$$End-to-End\ delay\ (s) = \sum Delay\ for\ each\ data\ packet \tag{2}$$

(3) **Total number of delivered data packets**: A ratio of the total received packets at the destination to the total packets generated by source node in the presence of both wormhole attack traffic and normal traffic.

$$Packet\ Delivery\ Rate = \frac{Packets\ received}{Packets\ generated} * 100 \tag{3}$$

The simulation parameters are shown in Table 1.

Table 1. : Simulation Parameters

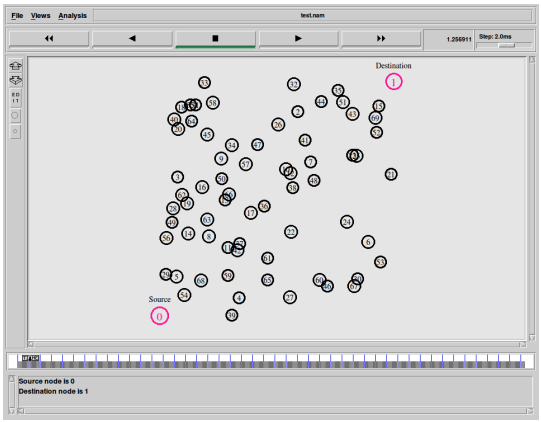
Simulator	NS-2
Number of nodes	1 40, 70, 100
Wormhole pairs	1 (Wormhole nodes 2)
Speed variation	10 ms
Area	1000 m x 1000 m
Communication range	250 m
Interface type	Phy/WirelessPhy
MAC type	IEEE 802.11
Queue type	Droptail/Priority Queue
Queue length	50 packets
Antenna type	Omni antenna
Propagation type	TwoRayGround
Routing protocol	AODV, TRM_AODV and APS_AODV
Transport agent	UDP
Application agent	CBR
Packet size	1024 bytes
Simulation time	100 s
Mobility model	RWP

5.2 Network Environment

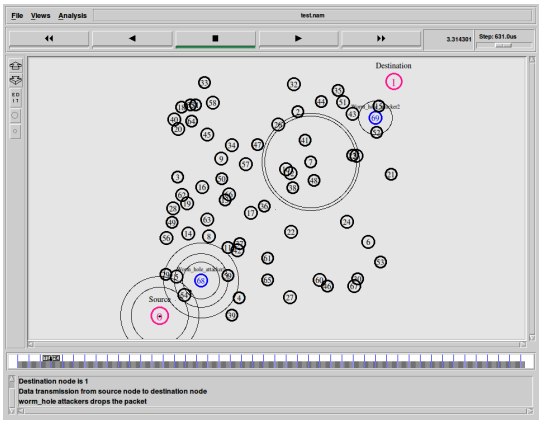
Figure 4 shows one sample of scenarios with 70 nodes ran in NS-2 environment. Figure 5a shows the throughput of the methods for three different number of nodes. The average performance of the proposed method with increasing the number of nodes is promising as compared to other methods. This confirms that the throughput of the given algorithm increases for dense networks. The average of delay is shown in Figure 5b.
According to the results, the average delay by increasing the number of nodes gets high for TRM_AODV, while the proposed method and the AOMDV method gets improved with less delay. However, there is still a performance gap between the wormhole detection and prevention algorithms and the attack-free channel in terms of delay. Finally, the average results for packet delivery ratio is depicted in Figure. 5c. The proposed algorithm attempts to keep a reasonable packet delivery ratio in presence of attack even by scaling the network size. The results confirms that the proposed algorithm outperformed other methods and still needs to be improved to be able to reach to the better packet delivery ratio as compared to attack-free channels. A future work is needed for active researchers.

6. CONCLUSION

Over the years, wireless sensor networks have gained much popularity, because of its operating nature in day to day use in wireless channels. Wormhole attack can significantly degrade network performance. The most previous research works have been focused on detecting this attack without preventing. In this paper, we proposed an improved algorithm to detect and eliminate further attack without any specialized hardware, implemented based on the modified AODV protocol in NS-2. This approach works by checking the validity of two hop neighbours that has forwarded the packet, an attack is detected when the identity of the two hop neighbours is found illegal. The authentication checks is carried out using a prestored nodes neighbour monitoring information. While the elimination of the malicious nodes is carried out using a hop count of previously route reply information. The accuracy of defence schemes are measured regarding throughput, delay, and packet delivery ratio. From the simulation results, it is observed that the proposed method provided promising results. In the future work, the plan should be based on the decreasing the false positive rate, where hidden wormhole attacks are launched.



(a) Before luanching attack



(b) During launched attack

Fig. 4: Network simulation in the presence of wormhole attack

7. REFERENCES

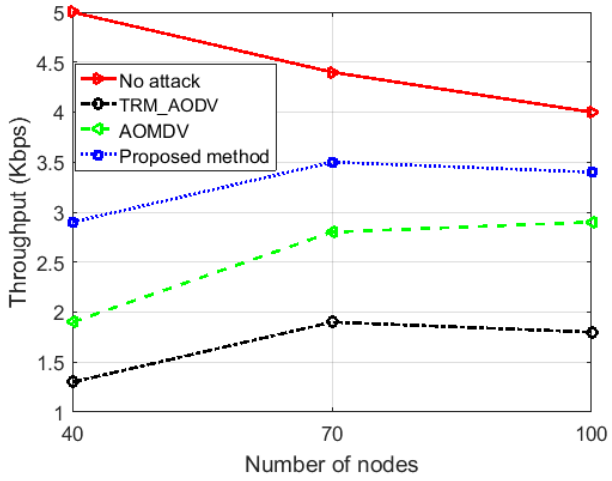
[1] Ravinder Ahuja, Alisha Banga Ahuja, and Pawan Ahuja. Performance evaluation and comparison of aodv and dsr routing protocols in manets under wormhole attack. In *Image Information Processing (ICIIP)*, pages 699 – 702, 2013.

[2] Parmar Amish and V.B. Vaghela. Detection and prevention of wormhole attack in wireless sensor network using aomdv protocol. *Procedia Computer Science*, 79:700 – 707, 2016.

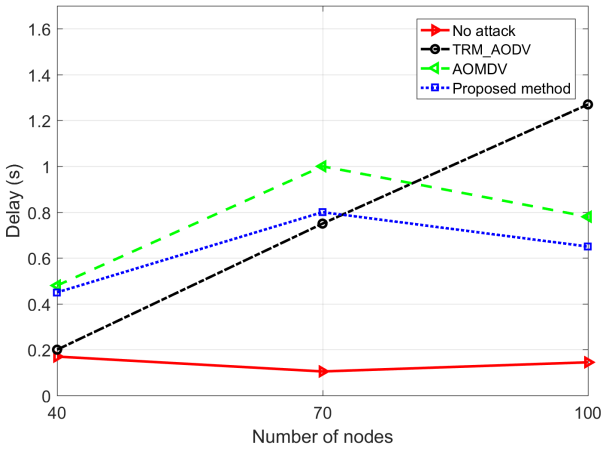
[3] Swati Bhagat and Trishna Panse. A detection and prevention of wormhole attack in homogeneous wireless sensor network. In *International Conference on ICT in Business Industry Government (ICTBIG)*, pages 1 – 6, 2016.

[4] J. Biswas, A. Gupta, and D. Singh. Wadp: A wormhole attack detection and prevention technique in manet using modified aodv routing protocol. In *9th International Conference on Industrial and Information Systems (ICIIS)*, pages 1 – 6, 2014.

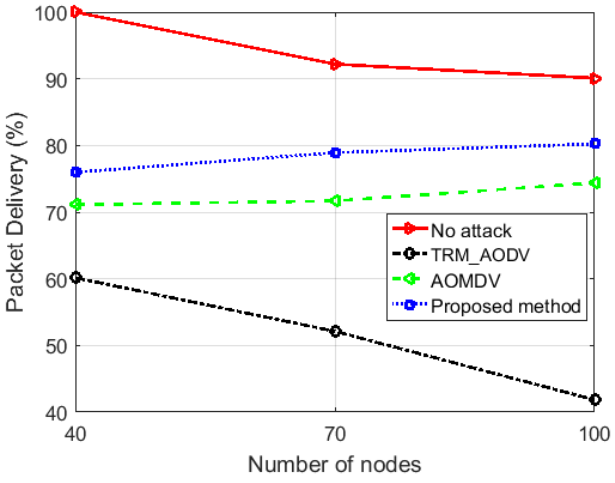
[5] Avinash S. Bundela. Literature survey on wormhole attack. *International Journal of Engineering Sciences & Research Technology*, 4(6):41 – 48, 2015.



(a) Throughput



(b) Delay



(c) Packet Delivery

Fig. 5: Average results for 40, 70 and 100 nodes

[6] Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux. Sector: Secure traking of node encouters in multi-hop wireless networks. In *Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS)*, pages 21 – 32, 2003.

[7] S. Choi, D. y. Kim, D. h. Lee, and J. i. Jung. Wap: Wormhole attack prevention algorithm in mobile ad hoc networks. In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008)*, pages 343 – 348, 2008.

[8] Saurabh Ganeriwal, Ram Kumar, and Mani B. Srivastava. Timing-sync protocol for sensor networks. In *Proceedings of the 1st international conference on Embedded networked sensor systems. ACM*, pages 138 – 149, 2003.

[9] Gaurav Garg, Sakshi Kaushal, and Akashdeep Sharma. Reactive protocols analysis with wormhole attack in ad-hoc networks. In *Computing, Communication and Networking Technologies (ICCCNT)*, pages 1 – 7, 2014.

[10] M. P. Gulwade, K. J. Dhoot, A. I. Bajaj, and M. M. Ghonge. Effectiveness of wormhole attack on dsr protocol in manet. *World Research Journal of Telecommunications Systems*, 1(1):13 – 15, 2012.

[11] Lingxuan Hu and David Evans. Using directional antennas to prevent wormhole attacks. In *NDSS*, 2004.

[12] Y. C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, volume 3, pages 1976 – 1986, 2003.

[13] Amin Karami. A framework for uncertainty-aware visual analytics in big data. In *Proceedings of the 3rd International Workshop on Artificial Intelligence and Cognition (AIC 2015)*, volume 1510, pages 146 – 155. CEUR-WS, 2015.

[14] Amin Karami and Manel Guerrero-Zapata. Mining and visualizing uncertain data objects and named data networking traffics by fuzzy self-organizing map. In *Proceedings of the 2nd International Workshop on Artificial Intelligence and Cognition (AIC 2014)*, volume 1315, pages 156 – 163. CEUR-WS, 2014.

[15] Amin Karami and Manel Guerrero-Zapata. An anfis-based cache replacement method for mitigating cache pollution attacks in named data networking. *Computer Networks*, 80:51 – 65, 2015.

[16] Amin Karami and Manel Guerrero-Zapata. A fuzzy anomaly detection system based on hybrid pso-kmeans algorithm in content-centric networks. *Neurocomputing*, 149(Part C):1253 – 1269, 2015.

[17] Amin Karami and Manel Guerrero-Zapata. A hybrid multi-objective rbf-pso method for mitigating dos attacks in named data networking. *Neurocomputing*, 151(Part 3):1262 – 1282, 2015.

[18] I. Khalil, Saurabh Bagchi, and N. B. Shroff. Liteworp: a lightweight countermeasure for the wormhole attack in multihop wireless networks. In *International Conference on Dependable Systems and Networks (DSN'05)*, pages 612 – 621, 2005.

[19] Pravin Khandare and N. P. Kulkarni. Public key encryption and 2ack based approach to defend wormhole attack. *India International Journal Of Computer Trends And Technology*, 4(3):247 – 252, 2013.

[20] A. Malhotra, D. Bhardwaj, and A. Garg. Wormhole attack prevention using clustering and digital signatures in reactive routing. In *Proceedings of 9th IEEE International Conference on Networking, Sensing and Control*, pages 122 – 126, 2012.

[21] Sergio Marti, Thomas J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 255 – 265, 2000.

[22] P. Sharma and A. Trivedi. An approach to defend against wormhole attack in ad hoc network using digital signature. In *IEEE 3rd International Conference on Communication Software and Networks*, pages 307 – 311, 2011.

[23] Sejun Song, Haijie Wu, and Baek-Young Choi. Statistical wormhole detection for mobile sensor networks. In *Fourth International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 322 – 327, 2012.

[24] Andreas Tonnesen. Reactive rotocols - AODV, 2004. `http://www.olsr.org/docs/report_html/node16.html`, accessed at 2017-05-20.

[25] Saurabh Upadhyay and Brijesh Kumar Chaurasia. Impact of wormhole attacks on manets. In *International Journal of Computer Science & Emerging Technologies*, pages 77 – 82, 2011.

[26] Guowei Wu, Xiaojie Chen, Lin Yao, Youngjun Lee, and Kangbin Yim. An efficient wormhole attack detection method in wireless sensor networks. *Computer Science and Information Systems*, 11(3):1127 – 1141, 2014.