EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

# A lightweight technique for detection and prevention of wormhole attack in MANET

Zulfiqar Ali Zardari[1], Kamran Ali Memon[2,*], Reehan Ali Shah[3], Sanaullah Dehraj[4], Iftikhar Ahmed[5]

[1] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China
[2] School of Electronic Engineering, Beijing University of Posts & Telecommunications, Beijing, China
[3] Department of computer system Engineering, faculty of Engineering, The Islamia University Bahawalpur, Pakistan
[4] Department of Mathematics and Statics, Quaid e Awam University of Engineering, Science and Technology, Nawabshah, Pakistan
[5] School of Computer science, Beijing Institute of Technology, China

## Abstract

A mobile ad-hoc network (MANET) is an ordinary and self-orbiting communication network that is capable of managing mobile nodes. Many proposed protocols on MANET address its vulnerability against different threats and attacks. The malicious node exploits these vulnerabilities to lunch attacks, especially when nodes have mobility and network do not have constant topology, like wormhole attack. This paper presents a lightweight technique that detects the wormhole attacks in MANET. In the proposed technique, the source node calculates the average sequence number of the reply (RREP) packets. If the sequence number of the corresponding node exceeds the calculated average value of the sequence number, then all traffic is discarded, and the node is marked as malicious. The proposed technique is less complex, power-efficient, and enhances network lifetime as more data packets are delivered to the destination node. This technique is validated through comprehensive simulations results in NS2

**Keywords:** MANET, Denial of service, Wormhole attack, Average sequence number, Reply (RREP) packet

Received on 16 May 2020, accepted on 04 July 2020, published on 08 July 2020



doi: 10.4108/eai.13-7-2018.165515

*Corresponding author. Email: Ali.kamran77@gmail.com

## 1. Introduction

Mobile Ad-hoc Network is a wireless network without any infrastructure which includes mobile nodes that can move according to a pattern, and the topological structure of the network keeps on changing dynamically. The routes between any two nodes are made through the intermediate hops on the ad-hoc basis, i.e., these routes are temporary and may disrupt with the passage of time due to several factors. Due to the dynamic nature of MANET is considered as a distributed network [1] in which a large number of nodes exchange information through symmetrical or asymmetrical radio links in a multi-hop manner. In MANET, nodes can act as intermediate hop or router to provide a route between two end nodes that can act in a spontaneous and ad-hoc manner. MANET network is used for disaster management, rescue operations, communicate through this path formed by intermediate nodes. These paths are formed using one of several standards or customized routing protocols following a specific mechanism linked to those protocols which can be categorized as proactive, reactive, and hybrid [2]. All these routing protocols might create a loophole in the security of the network due to their intrinsic properties. All these features of MANET pave the way for a wide range of both active as well as passive attacks [3] that makes the issue of data security of critical importance. Even with these drawbacks, MANET has the bulk of features that makes it successful in various fields. MANET finds its application in the field where it is difficult to set up a wired network with centralized or decentralized infrastructure with fixed base stations around which the entire network is controlled [4]. MANET proves to be handy on these occasions as it involves mobile nodes that build paths and communicate military communication services, short-range communications, etc. reason it is very cheap as compared

to a wired network. Because no wires are deployed, all nodes are wireless [5]. In the existing work, the trust calculation is performed based on the number of packets sent or received generated by nodes. It is not only the situation to measure trust due to passive attacks [6]. Also, the attacker node only senses data or modifies then transfers the information to other malicious nodes again and again. Due to this, it split the security strategy of a trustworthy AODV routing protocol relevant to detecting or preventing MANET malicious behavior of the nodes. Trust state does not rely on receiving packets or forwarding other packets, but trust is a different technique to overcome all types of passive and active attacks. Among other problems in MANETs, the security of mobile nodes is a major challenge, because every node is free in MANET. Security is also a problem because there is a lack of a centralized control unit due to the MANET's infrastructure less environment [7]. Therefore, an efficient and safe mechanism is required to ensure the maximum efficiency and security of transmission of packets in the path between nodes.

Two or more malicious nodes typically initiate a wormhole attack using a private tunnel channel, between them. Figure 1 shows the workings of the wormhole attack. A malicious node at one end of the tunnel catches a control packet and sends it through a private channel to another colluding node at the other end, which retransmits the packet locally. The attack usually works in two steps. The wormhole nodes get involved in several routes during the first step. Those malicious nodes start exploiting the packets they receive in the second step[8].

These nodes can, in many ways, interrupt network functionality. For example, such nodes may confuse protocols that rely on node position or geographic proximity, or in the case of virtual tunnels, the colluding nodes may forward data packets back and forth to each other to exhaust the battery of other intermediate nodes. Wormhole nodes can drop, change, or send data for malicious purposes to a third party [9].

DoS attacks are aggressive attacks where malicious nodes produce false messages to interrupt the operations of the network, or consume the resources of other nodes. In MANET, Wormhole, Blackhole, Gray hole, Jellyfish, etc. are well known DoS [10][11]

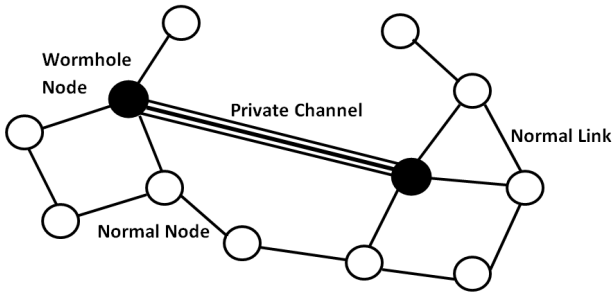


**Figure 1.** Wormhole attack in MANET

In this paper, we proposed a technique which detects the wormhole attack by using sequence number. In the proposed technique, the source node temporarily stores all replies (RREP) packets from other nodes with their sequence numbers. Then source node (S) calculates the average of all sequence numbers and stores it. After calculating the average, it discards all replies packets if the sequence number of any node exceeds the average value S. In this way, wormhole nodes can be excluded from the route, and only trusted nodes can communicate in the network. Contribution of the research follows:

(i). The proposed technique is lightweight, which detects the wormhole nodes in very little complexity. In order to achieve accurate attack detection and security assessment, the proposed technique provides a simple and less complicated solution to identify the malicious as compared to existing solutions.

(ii). Due to the rapid detection of wormhole attack of the proposed technique, causes an increase in packet delivery ratio and throughput of the network.

(iii). The proposed technique does not create extra overhead in the network.

Table 1. Existing solution year wise

| S.No. | *Author & year* | *Detection Task* | *Detection technique used* | *Protocol* |
|---|---|---|---|---|
| 01 | L. Buttyan (2005) [12] | Wormhole attack | Neighbor Number test | Distance bounding |
| 02 | S. Choi (2008) [13] | Wormhole attack | Wormhole attack prevention | DSR |
| 03 | M. Azer (2009) [14] | Wormhole attack | Complex Wormhole attack | AODV |
| 04 | S. Gupta (2011) [15] | Wormhole attack | Wormhole hound packet | AODV |
| 05 | A. Vani (2011) [16] | Wormhole attack | Hop count based | AODV |
| 06 | U. Kumar (2012) [17] | Wormhole attack | Modified AODV | AODV |
| 07 | Z. Khan (2012) [18] | Wormhole attack | Modified routing table | DSDV |

| | | | | |
|---|---|---|---|---|
| 08 | M M. García-Otero (2012) [19] | Wormhole attack | Localization | Geographical |
| 09 | V. F. Taylor (2013) [20] | DoS attack | AI and the CLIPS expert system | AODV |
| 10 | S. S. Sahu (2014) [21] | DoS attack | Traffic filtering | AODV |
| 11 | R. Upadhyay (2015) [22] | DDoS attack | Battery drain | AODV and DSR |
| 12 | M. Bendjima (2016) [23] | Wormhole attack | Mobile agents | AODV |
| 13 | D. Goyal (2016) [24] | Wormhole attack | dempster shaper theory | AODV |
| 14 | M. Kumar (2017) [25] | Wormhole attack | Data Aggregation | Greedy Perimeter Stateless Routing Protocol |
| 15 | F. Aslam khan (2017) [26] | Wormhole attack | Special (DPS) nodes | AODV |
| 16 | Josia Antony (2018) [27] | Malicious nodes | Single directional antenna | AODV |

## 2. Related Work

In the above literature, various solutions are based on trust and threshold values which detects the wormhole nodes. However, these solutions create high routing overhead and delay in the network. Additionally, some techniques have computational complexity and required extra hardware, which affects the standard routing protocol and increases the cost [28], [29].

The main problem, the literature identifies is the improper detection of malicious nodes and huge routing overhead in the network; this work motivates us to propose this technique. Many researchers focus only on the packet delivery ratio but ignore the routing overhead and delay.

Our proposed technique is different from all the above exiting solutions, which does not require any extra hardware or computational complexity. The proposed technique is a less complicated and lightweight solution because, based on the average value of sequence numbers, identifies the wormhole nodes in the network.

## 3. Proposed Methodology

Most of the defending strategies use intermediate nodes to prevent attacks or uses some techniques such as intrusion detection systems (IDS) to detect malicious nodes. Where this solution becomes more complicated, expensive, and it also decreases the lifetime of the network [30]. In this paper, we have suggested a defensive method in this article that is very simple to enforce and will protect against wormhole attacks. In our proposed solution, the source node accepts various reply (RREP) packets from different nodes, all RREP packets (for a specific moment) will be stored by the sender with their respective sequence numbers. Then the corresponding node calculates the average number of all sequence numbers.

$$avg = (a_1 + a_2 + \cdots + a)/n$$

Here (n) represents the total number of reply (RREP) packets whereas a1, a2 …. an is the sequence number of reply (RREP) packets. Discard all reply (RREP) packets that exceed the value of avg with a sequence number.

The Pseudocode of the proposed technique

Calculate:

$avg = (a_1 + a_2 + s_2 + \cdots + a[n])/n\,;$

For all $i$ where $i = n\ to\ 1$

If (sequence number$[i] > avg$)

Discard that path, node is (wormhole node)

Set $i = i - 1$;

Else

Choose the path to send the data

End for

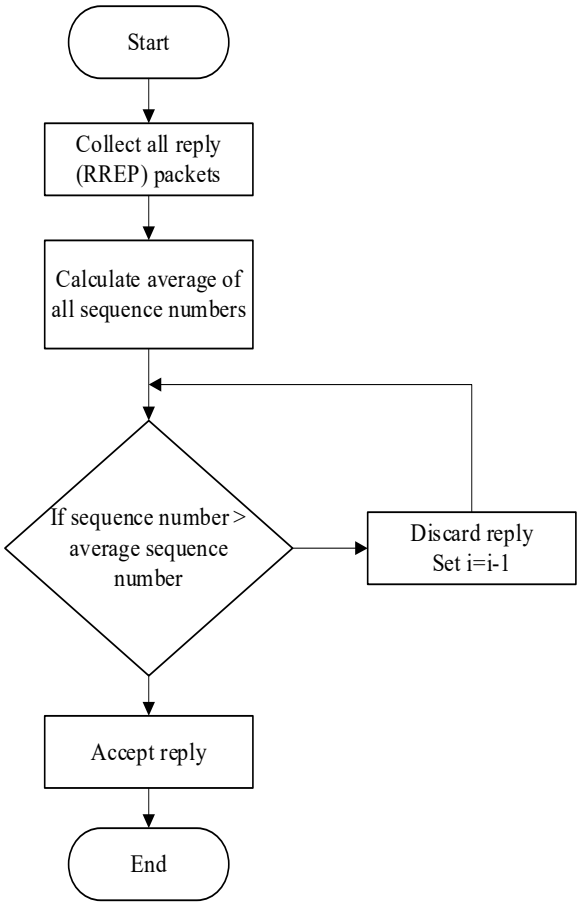


**Figure 2.** Proposed technique flowchart

Security of the nodes is the key aspect of the Mobile ad hoc network, especially the DoS attack exploits vulnerabilities to damage valuable resources of the network. The proposed technique successfully defended the wormhole attack with less routing overhead. This technique increases network lifetime and saves the battery power of the wireless nodes.

Table 2. Simulation Parameters

| PARAMETERS | VALUE |
|---|---|
| Network Simulator | NS-2(ver.2.34) |
| Dimension | 1000× 1000 m |
| Regular nodes | 40 |
| Mobility model | The random walk mobility model |
| Simulation time | 1000 s |
| Traffic type | CBR/UDP |
| Packet size | 512 bytes |
| Mobility speed | 0.5-01m/s |

## 4. Results and Discussion

### 4.1. Packet Delivery ratio

Fig.3 shows the result of the packet delivery ratio of the proposed technique and simple AODV with & without attack. The PDR of AODV with an attack is very low, because the malicious node drops the data packets during communication. The PDR of AODV without attack is very high due to the malicious node does not exist in the network. Moreover, PDR of the proposed technique is higher than AODV with attack and less than simple AODV. This shows that the rapid detection of a malicious node by the status packet increases PDR. However, PDR decreased by either a link failure or a malicious node, where the malicious node is close to the source node and sends false information to the source node more quickly.

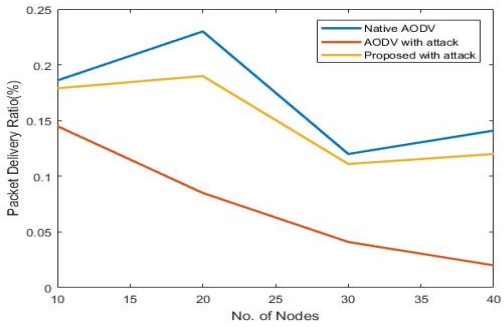


**Figure 3.** Packet delivery ratio

### 4.2. Throughput

Fig.4 shows the result of the throughput of the proposed technique and simple AODV with & without attack. The throughput of AODV with an attack is low because the malicious node disturbs the communication. Whereas, the throughput of AODV without attack is high because no malicious node is found, and nodes can communicate freely. Similarly, the throughput of the proposed technique is better than AODV with attack and less than simple AODV. However, throughput of the proposed technique is decreased; either when the link inflicted failure during communication, or when the malicious node dropped the data packets.

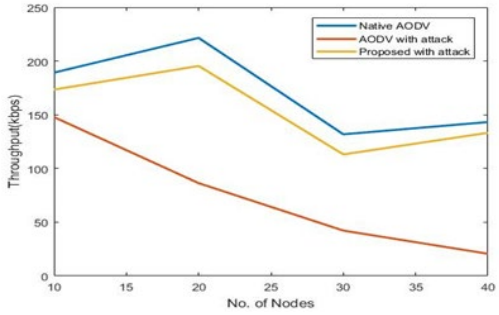


**Figure 4.** Throughput

## 4.3. Average delay

Fig.5 shows the result of the average delay of the proposed technique and simple AODV with & without attack. The delay of AODV with an attack is low. Therefore, data packets cannot reach a destination node within due time. The performance of AODV without attack is better than both simple AODV and proposed technique. There is no disturbance of the attacker node, whereas the proposed technique is better than simple AODV and less than AODV under attack.

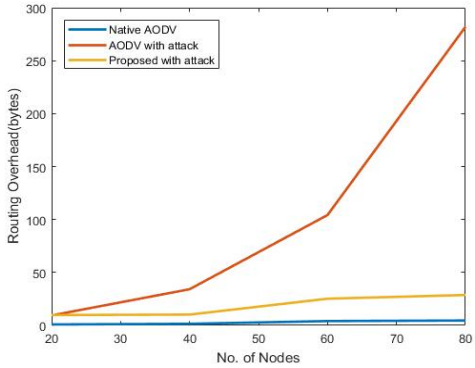


**Figure 5.** Average Delay

## 4.4. Routing overhead

Fig.6 shows the routing overhead of the proposed technique, native AODV, and AODV with the attack. Routing overhead of AODV is very low because there is no attack, whereas, in the proposed technique, overhead is minimum as compared to AODV with the attack.

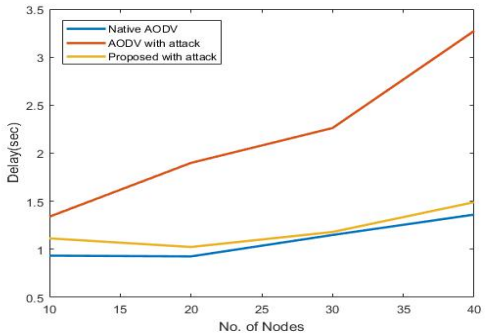


**Figure 6.** Average Delay

## 5. Conclusion

Security is one of the critical aspects of the network of wireless communication. During communication, DoS attacks disturb the routing process and damage the network resources. Wormhole attack is difficult to detect because it creates the tunnel to drop the data packets. In this paper, we have proposed a lightweight technique to detect the wormhole nodes based on calculating the average sequence number with very delay in the network. Hence, the rapid detection of wormhole nodes saves the battery of the nodes, which helps to increase the network lifetime. In the future, we will deploy this technique to other routing attacks by considering the mobility of the nodes. The proposed work is limited only to detect the wormhole attacks.

In the future, the proposed can merge with machine learning techniques for the detection of malicious nodes. Furthermore, the proposed technique can be extended by calculating the energy consumption of the nodes during the transmission phase.

## References

[1] S. Majumder and D. Bhattacharyya, *Mitigating wormhole attack in MANET using absolute deviation statistical approach*. 2018.

[2] R. Verma, R. Sharma, and U. Singh, *New approach through detection and prevention of wormhole attack in MANET*. 2017.

[3] C. Gupta and P. Pathak, "Movement based or neighbor based tehnique for preventing wormhole attack in MANET," in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016, pp. 1–5.

[4] D. Sharma and R. Kumar, *Reviewing the impact of wormhole attack in MANET*. 2016.

[5] H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap, and K. Wandra, *Advanced AODV approach for efficient detection and mitigation of wormhole attack in MANET*. 2016.

[6] S. Parbin and L. Mahor, *Analysis and prevention of wormhole attack using trust and reputation management scheme in MANET*. 2016.

[7] P. Sharma and V. Sharma, *Survey on security issues in MANET: Wormhole detection and prevention*. 2016.

[8] H. Mishra and M. Mittal, "Analysis of Wormhole Attack on AODV and DSR Protocols Over Live Network Data," 2020, pp. 681–690.

[9] P. Kaur, D. Kaur, and R. Mahajan, "Wormhole Attack Detection Technique in Mobile Ad Hoc Networks," *Wireless Personal Communications*, vol. 97, Jul. 2017.

[10] P. K.K, A. Laghari, and R. Laghari, "A Step towards the Efficiency of Collisions in the Wireless Sensor Networks," *ICST Transactions on Scalable Information Systems*, vol. 0, no. 0, p. 159409, 2018.

[11] R. Jhaveri, S. Patel, and D. Jinwala, *DoS Attacks in Mobile Ad Hoc Networks: A Survey*. 2012.

[12] L. Buttyan, L. Dóra, and I. Vajda, *Statistical Wormhole Detection in Sensor Networks*. 2005.

[13] S. Choi, D. Kim, D. Lee, and J. Jung, *WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks*. 2008.

[14] M. Azer, S. El-Kassas, and M. El-Soudani, "A Full Image of the Wormhole Attacks - Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks," vol. 1, Jun. 2009.

[15] S. Gupta, S. Kar, and D. Selvamuthu, *WHOP: Wormhole attack detection protocol using hound packet*. 2011.

[16] A. Pradesh and D. S. Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for

Secure Routing In Ad Hoc Wireless Networks," vol. 3, no. 6, pp. 2377–2384, 2011.
[17] U. Chaurasia and V. Singh, *MAODV: Modified wormhole detection AODV protocol*. 2013.
[18] Z. Khan and M. Islam, *Wormhole attack: A new detection technique*. 2012.
[19] M. García-Otero and A. Población-Hernández, "Detection of wormhole attacks in wireless sensor networks using range-free localization," in *2012 IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2012, pp. 21–25.
[20] V. Taylor and D. Fokum, *Securing wireless sensor networks from denial-of-service attacks using artificial intelligence and the CLIPS expert system tool*. 2013.
[21] S. Bilgaiyan, S. Sahu, and P. Priyadarshini, *Curbing Distributed Denial of Service attack by traffic filtering in Wireless Sensor Network*. 2014.
[22] R. Upadhyay, U. Bhatt, and H. Tripathi, "DDOS Attack Aware DSR Routing Protocol in WSN," *Procedia Computer Science*, vol. 78, pp. 68–74, Dec. 2016.
[23] M. Bendjima and M. Feham, "Wormhole attack detection in wireless sensor networks," in *2016 SAI Computing Conference (SAI)*, 2016, pp. 1319–1326.
[24] D. Goyal and A. Parashar, "Trust computation using D-S in sector based area to detect or preventing worm hole in MANET," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2016, vol. 1, pp. 1–5.
[25] M. K. and K. Dutta, "Detecting Wormhole Attack on Data Aggregation in Hierarchical WSN," *International Journal of Information Security and Privacy (IJISP)*, vol. 11, no. 1, p. 17, 2017.
[26] F. Khan, M. Imran, H. Abbas, and H. Durad, "A Detection and Prevention System against Collaborative Attacks in Mobile Ad hoc Networks," *Future Generation Computer Systems*, vol. 68, Oct. 2016.
[27] J. Antony and K. S. Adarsh, *A Survey on computation of neighbouring nodes and malicious nodes in all direction with single directional antenna*. 2018.
[28] N. Seresht, Y. Miao, S. Michalska, Q. Liu, and H. Wang, "From logs to stories: human-centred data mining for cyber threat intelligence," IEEE Access, vol. PP, p. 1, Jan. 2020.
[29] R. Rasool, U. Ashraf, K. Ahmed, H. Wang, W. Rafiq, and Z. Anwar, "CyberPulse: A Machine Learning based Link Flooding Attack Mitigation System for Software Defined Networks," IEEE Access, vol. PP, p. 1, Mar. 2019.
[30] G. Kim, C. Serban, and R. Chadha, Attack-Resistant Routing : a Framework for Enhancing Routing Robustness in Wireless Ad-hoc Networks. 2020.