Int. j. inf. tecnol. (June 2020) 12(2):539–546
https://doi.org/10.1007/s41870-019-00417-4

ORIGINAL RESEARCH

RTT based wormhole detection for wireless mesh networks

Amit Kumar Roy[1] · **Ajoy Kumar Khan**[1]

Received: 6 February 2019 / Accepted: 30 December 2019 / Published online: 25 January 2020

Abstract One of the challenging security threats to wireless mesh network (WMN) is their vulnerability to routing protocols. This vulnerability is mainly caused by certain internal attacks, one of which is known as a wormhole attack. This attack is launched by two or more malicious nodes which gives a false illusion of shortest path through them via a tunnel. They formed a tunnel via encapsulation, which restricts the increment of hop count during the traversal through intermediate nodes and therefore launches a wormhole attack between source and destination. In this paper, we proposed a detection mechanism based on the calculation of round trip time (RTT) and processing time to identify the malicious nodes forming wormhole attack. Our proposed work prevents the AODV routing protocol against the wormhole attack in WMNs. The simulation of our proposed work had done using NS-3 simulator, and the results show that the performance of our detection algorithm improves over the existing detection techniques against wormhole attack.

Keywords Mesh network · Wormhole attack · Round trip time (RTT) · Processing time · Threshold value

✉ Amit Kumar Roy
amitkroy12@gmail.com

Ajoy Kumar Khan
ajoyiitg@gmail.com

[1] Department of Computer Science and Engineering, Assam University, Silchar, India

1 Introduction

Wireless mesh networks (WMNs) has emerged as a key technology for next-generation wireless networks due to its self-organizing, self-configuring and minimal upfront investment in deployment. WMNs have divided into three tiers, the top-tier consists of gateway routers, the middle-tier is also known as the backbone of WMNs consists of mesh routers (MRs), and the bottom-tier consists of mesh clients (MCs). Gateway routers are connected to the Internet through wired networks, the mesh routers (MRs) also act as access points (APs) in the backbone are connected to the gateway routers using multi-hop communication [1, 2]. Therefore, when a mesh client wants to get access to the Internet, it sends its request to MRs and then the MRs forwards the request towards the gateway router in a multi-hop fashion [3]. However, due to the distributed nature of WMNs certain attacks can be launched easily in WMNs, one of which is known as wormhole attack [4]. The wormhole attack can be launched in various modes which include using high power transmission, tunneling using encapsulation and out-of-band channels [5]. All the three modes of attacks allow the transmitted packets to reach faster with a minimum number of hops towards the destination compared to normal multihop routes. These attacks formed a fake illusion that the two end point of the tunnel is very close to each other, hence the normal nodes are attracted towards this tunnel and forward the packets with minimum hops. The packets through the tunnel then can be selectively dropped or controlled by the malicious nodes. The wormhole attack violates the legal operation of AODV routing protocols and prevents the two nodes from discovering legitimate routes and thus disrupt network functionality.

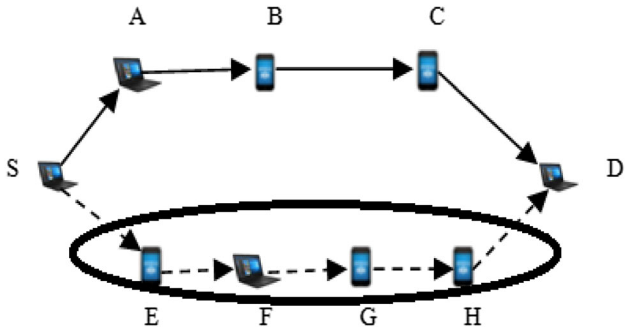


Fig. 1 Wormhole tunnel formed between S and D

Figure 1 shows the wormhole tunnel formed by malicious nodes E and H. Assume that mesh nodes S and D are far apart against each other. In the above figure, it can be seen that there are two possible routes from S to D. One is (S–A–B–C–D) normal route with a hop count of 4 and second route is via a tunnel (S–E–H–D). By transmitting packets from malicious nodes E to node H through the tunnel, it convinces the sender node S to believe that the receiver node D is nearer to S with a hop count of 3. The malicious nodes E and H replay packets to each other via wormhole tunnel and make a false illusion of shortest path towards the destination node D; therefore selectively drop out the data packets or control the packets in order to disrupt the communications between mesh nodes S and D. Security is, therefore an issue of prime importance in WMNs. A secure routing protocol for forwarding data packets between mesh nodes is required for WMNs. Therefore, to enforce secure cooperation and coordination among mesh nodes, various collaboration schemes had proposed in the literature [6] to detect the malicious nodes in the networks. Several mechanisms had proposed that are based on a hardware device and frameworks to trust and believe the nodes in the networks and attempt to identify malicious nodes by suitable decision making systems and then isolate or punish them [7].

In this paper, we propose a wormhole detection algorithm that is based on the calculation of round trip time (RTT) and processing time. We calculate the delay probability of sending and receiving packets between intermediate nodes (i.e., per hop) for each complete route between source to destination. Our proposed algorithm is mainly designed for the detection of malicious nodes to prevent AODV routing protocol against wormhole attack in WMNs.

1.1 AODV routing protocol

Assume that a route has to construct from source S to destination D. At the initial state node S broadcast the route request packet (RREQ) over the network as shown in Fig. 2. Similarly, the intermediate nodes will broadcast the RREQ until it reaches the destination node D. A destination node D after receiving the RREQ, reply back with a route reply message (RREP) in a unicast fashion in reverse order. During the transmission of both RREQ and RREP, the routing table at each node is updated with the information of route setup. If the distance between source and destination is via relay nodes then the RREQ is forwarded among relay nodes with the increment of hop count in RREQ packet. Likewise, after RREQ arrives to the destination D, the destination node prepares a RREP packet and forwards it in a reverse order via relay nodes towards the source S as shown in Fig. 3. Finally, the route with minimum hop is chosen from source to destination.

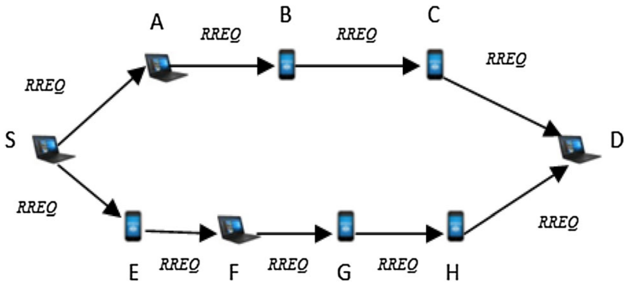


Fig. 2 AODV RREQ packet

2 Related works

This section highlights the previous works implemented to prevent the wormhole attacks in various wireless networks. Some of the existing work depends on special kind of hardware and some depend totally on efficient software design to resist the wormhole attacks. In this section, we have highlighted some existing works that are relevant to our proposed work.

Dromard et al. [8] proposed a protocol based on the extension of the existing watchdog scheme. The protocol detects the malicious behavior of the nodes that deny forwarding the packets towards the destination. The protocol

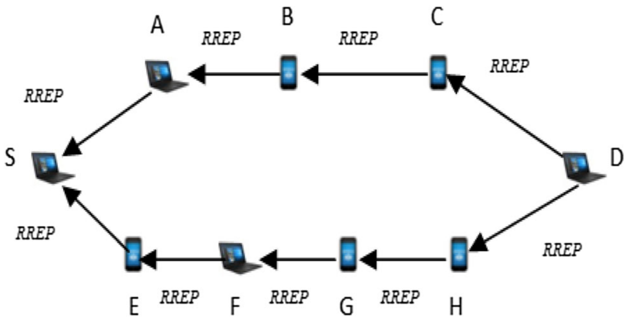


Fig. 3 AODV RREP packet

detects the misbehaving nodes in WMNs via certain performance metrics such as packet drop and acknowledgment. Capkun et al. [9] proposed a wormhole detection method where the nodes authenticate its neighbor based on one-bit challenge. Each node x sends a one bit challenge to node y, which node y responds immediately. The author employs a special hardware module to examine the delay process relevant to the respond of one-bit challenge. Delay in the response of one-bit challenge, enables the hardware to identify the malicious node in the network. Dias et al. [10] proposed a watchdog mechanism that detects the misbehaving nodes based on the performance of nodes in the network. The malicious node results in the delay of forwarding packets and drops or controls the packets. Their work analysis the delay of transmission packets occurred between cooperative nodes and identifies the malicious node over the network. Biswas et al. [11] had proposed an authentication method for the detection of wormhole attack. The authentication process detects the malicious nodes with their exact location and eliminates the chances of false positive results that arise during the detection of wormhole attack. Liu et al. [12] proposed a watchdog method for the detection of wormhole attack. The protocol is based on observer prototype and a finite state machine which identifies the misbehaving nodes with the change in the state program. Patel and Aggarwal [13] proposed a two-phase detection protocol to identify the wormhole attack and isolate them from the network. This protocol is based on two performance metrics, i.e., packet delivery ratio and throughput. Su [14] proposed WARP a secure routing protocol against wormhole attacks. WARP is an extension of AODV routing protocol where each node records the anomaly values of its neighbor's. WARP offers multi-path routing between nodes along with the detection capability of wormhole nodes. WARP detects the wormhole nodes when the link between the two nodes exceeds the threshold value and then discards that link from the network.

Cho et al. [15] proposed a protocol that secures against internal attacks that reside in a trust mechanism. The author identifies all the vulnerabilities of the trust mechanism and proposed a method to strengthen the detection capability of a trust mechanism known as a watchdog. Hern´andez-Orallo et al. [16] proposed Collaborative Contact-based Watchdog protocol known as CoCoWa. The protocol is based on the distribution of local monitor nodes that operates continuously when contact is made to it. The monitor nodes store all the information of selfish nodes and broadcast it over the network to other nodes about its presence. Wang et al. [17] proposed end-to-end detection method for a multi-hop route management based on a scheme called cell-based open tunnel avoidance (COTA). This information detects the malicious nodes in the neighboring relations. Qian et al. [18] proposed statistical analysis of multipath (SAM) protocol based on the analysis of routing statistics. The protocol detects the wormhole links between two nodes when the links exceed its frequency beyond the expected value. Matam et al. [19] proposed WRSR a secure routing protocol against wormhole attacks. The protocol detects the presence of misbehaving nodes during the route discovery process and isolates them from the network. The protocol is based on performance metrics called packet delivery ratio during the route discovery process. Luan et al. [20] proposed a wormhole detection protocol based on two concepts- watch nodes based detection and identity-based cryptosystem. The protocol employed threshold value where the packet drop ratio between two nodes exceeding the threshold value is considered as wormhole link. Shamieh et al. [21] proposed an adaptive compression technique (ACT) to improve the latency and packet drop ratio over the wireless network. The protocol is based on the observation of RTT and the packet delivery ratio during the transmission of data packets.

Shams et al. [22] proposed intrusion detection system (IDS) based on a vector machine algorithm to resist the malicious nodes in the network. The IDS monitors the data traffic transmitted over the network between intermediate nodes and detects the malicious behavior of the nodes based on the packet delivery ratio performed by the nodes. Abdel-Azim et al.[23] proposed an intrusion detection system based on the fuzzy system to ensure security against Black-hole and Gray-hole attacks. For optimization of the Fuzzy Inference System (FIS) the protocol employed adaptive neuro-fuzzy inference system (ANFIS) by using Genetic Algorithm (GA). Tran et al. [24], proposed Transmission Time based Mechanism (TTM) to resist wormhole attack to secure AODV routing protocol. The TTM is based on the calculation of RTT between intermediate nodes with constant transmission rate over the network. However, TMM suffers from vulnerabilities such as detecting wrong wormhole link in the presence of multi-rate transmission.

3 Tran et al.'s protocol

In this section, we shall review Tran et al. detection mechanism [24] and present our analysis of their proposed protocol.

In TTM, the AODV routing protocol is secured against wormhole attack. TTM allows the calculation of RTT between nodes during the establishment of the route from source to destination. Firstly, during the route discovery process, the RTT of each node along the route is calculated as the time taken to forward the route request (RREQ) towards the destination plus the time taken to receive the route reply packet (RREP) from the destination. Each node appends its RTT value in RREP packet and forwards to the source in reverse order. Secondly, the source node after receiving all the RTTs of each node compute the RTT between two nodes along the route as RTT of first node minus RTT of the second node, RTT of second node minus RTT of the third node and so on. Lastly, the source node compares the difference between the old RTTs and new RTT of each node and detects the wormhole link if the old RTT – new RTT value exceeds the threshold value which is assumed as 45 ms by the author. RREQ packet size (4 bytes) and RREP packet size (4 bytes) plays an important role during the calculation of RTT as it results in memory utilized for allocating the information of sending RREQ and receiving RREP at each node. In TTM the memory utilized by each node is given as n × (4 + 4) where n is the maximum number of RREQ received at each node at the same time. In TTM, n value is considered to 4, therefore, the memory utilized along each node is computed as 4 × (4 + 4) = 32 bytes. Figure 4 below shows the complete procedure of Tran et al. protocol for the setup of the route from source S to destination D.

Step 1: TS_{REQ}, $TA_{REQ,}$ $TB_{REQ,}$ and TC_{REQ} to destination D is the time of node S, A, B, C to forward RREQ. TD_{REQ} is not included as it is the destination.

Step 2: $TC_{REP,}$ $TB_{REP,}$ $TA_{REP,}$ and TS_{REP} to source S is the time of nodes C, B, A, S to receive RREP.

Step 3: RTT of node S, A, B, C with destination D is calculated as

RTTS, D = TSREQ + TSREP.
RTTA, D = TAREQ + TAREP.
RTTB, D = TBREQ + TBREP.
RTTC, D = TCREQ + TCREP.

Step 4: RTT between two successive nodes along the path is calculated as

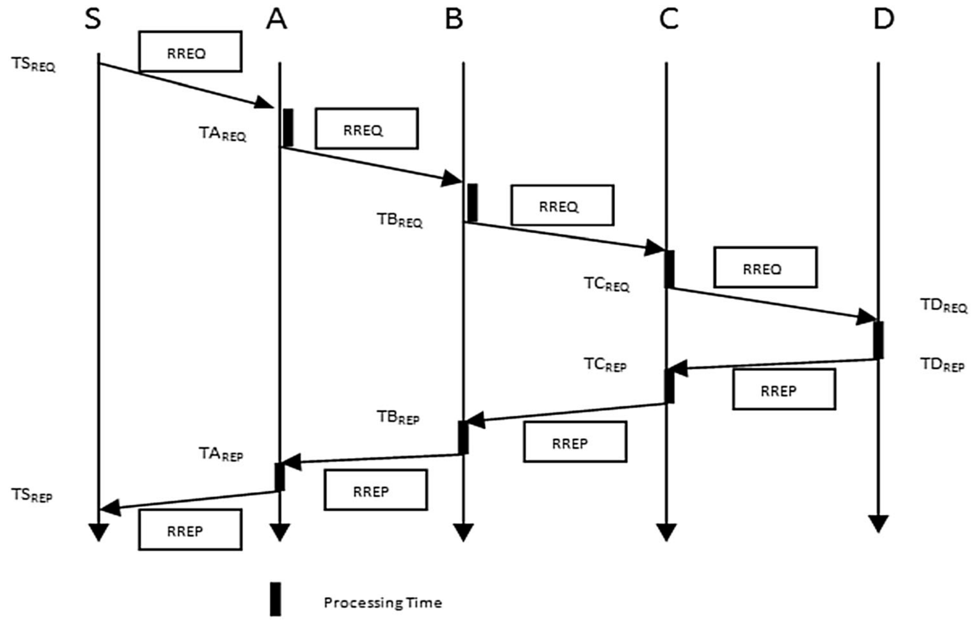
RTTS, A = RTTS, D—RTTA, D
RTTA, B = RTTA, D – RTTB, D
RTTB, C = RTTB, D – RTTC, D

3.1 *Analysis of Tran* et al.*'s protocol*

Tran et al.'s protocol suffers from certain vulnerabilities as follows:

1. In TTM, the detection of wormhole link is successful only under the consideration of constant rate transmission. However, in wireless networks, the transmission rates vary upon the change in network capacity and network conditions. Therefore, TTM fails to detect the wormhole link under multi-rate transmission which leads to incorrect detection of wormhole link.
2. Considering the calculation of RTT several times to obtain the average delay of RTT between the nodes. However, in the wireless network, the delay in RTT may be occurred due to processing time at the nodes.
3. As each node records the RREQ forwarding time and RREP receiving time, any malicious node along the path could alter these times and forward the false RTT information to the source.

Fig. 4 RREQ and RREP timing



4 Proposed protocol

To solve the above problem we proposed a detection mechanism based on the calculation of RTT in conjunction with propagation time which was not considered in Tran et al. protocol. To compute the processing time (PT), each node in the network records its RREQ forward time (TN_{REQ_F}) and RREQ receive time (TN_{REQ_R}) as well as RREP forward time (TN_{REP_F}) and RREP receive time (TN_{REP_R}) where TN is the transmission time of node N. In our proposed protocol the memory utilized by each node is given as n x (4 + 4 + 16) where 16 bytes are required to carry the processing time. If n = 5 then memory utilized at each node is 5 × (4 + 4 + 16) which equals to 120 bytes. Figure 5 shows the complete procedure of our proposed work from source S to destination D.

Step 1: TS_{REQ_F}, TA_{REQ_F}, TB_{REQ_F}, and TC_{REQ_F} is the time of node S, A, B, C to forward RREQ. TD_{REQ_F} is not included as it is the destination.

Step 2: TC_{REP_R}, TB_{REP_R}, TA_{REP_R}, and TS_{REP_R} is the time of node C, B, A, S to receive RREP.

Step 3: RTT of node S, A, B, C with destination D is calculated as

RTTS, D = $TS_{REQ_F} + TS_{REP_R}$

RTTA, D = $TA_{REQ_F} + TA_{REP_R}$

RTTB, D = $TB_{REQ_F} + TB_{REP_R}$

RTTC, D = $TC_{REQ_F} + TC_{REP_R}$

Step 4: RTT between two successive nodes along the path is calculated as

RTTS, A = RTTS, D—RTTA, D

RTTA, B = RTTA, D – RTTB, D

RTTB, C = RTTB, D – RTTC, D

Step 5: Processing time at node A, B, and C along the path is calculated as

$PT_A = TA_{REQ_F} - TA_{REQ_R}$ (RREQ processing time at node A).

$PT_A = TA_{REP_F} - TA_{REP_R}$ (RREP processing time at node A).

$PT_B = TB_{REQ_F} - TB_{REQ_R}$ (RREQ processing time at node B).

$PT_B = TB_{REP_F} - TB_{REP_R}$ (RREP processing time at node B).

$PT_C = TC_{REQ_F} - TC_{REQ_R}$ (RREQ processing time at node C).

$PT_A = TA_{REP_F} - TA_{REP_R}$ (RREP processing time at node C).

Algorithm

```
1. Randomly select nodes in wireless mesh networks.
2. Source node computes all the RTT of each node along the path towards the destination node.
3. Compute the PT of RREQ and RREP at each node.
4. Compute the TT of RREQ and RREP at each node.
5. Compute the old RTT = ($TT_N + PT_N$)
6. Compare new RTT with old RTT
if | new($RTT_{N_iN_{i+1}}$) – old ($RTT_{N_iN_{i+1}}$) | ≤| µ | then
No wormhole
else
Wormhole detected between node $N_i$ and node $N_{i+1}$
end if
```

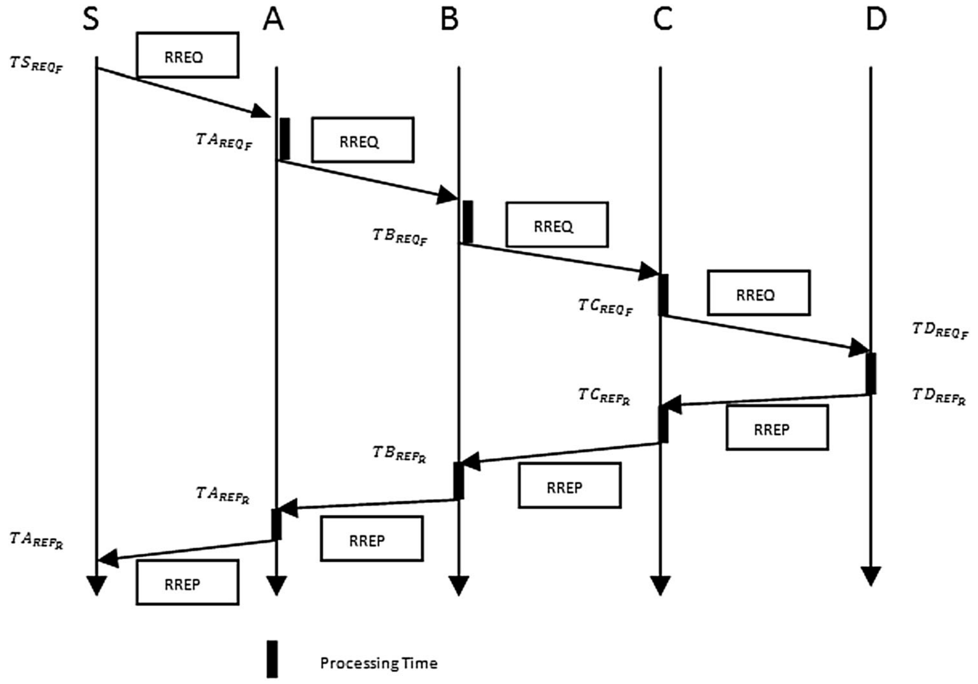


Fig. 5 RREQ and RREP timing of proposed work

Table 1 Experimental model setup

Parameters	Values
Simulator	NS-3.21
Simulation area	1000 × 1000 m
MAC layer protocol	IEEE 802.11
No. of mesh nodes	10, 20, 40, 60
Transmission range	250 m
Routing protocol	AODV
Node placement	Random
Simulation time	100 s

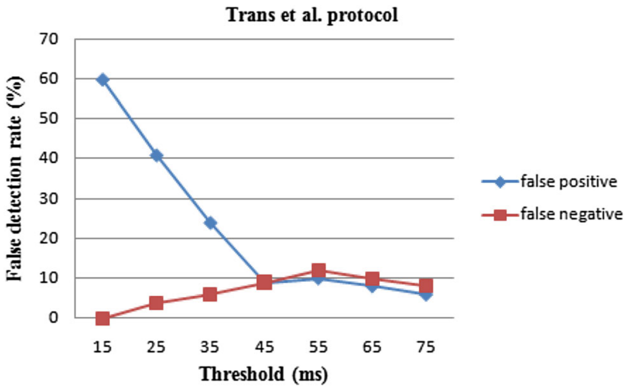


Fig. 6 False detection rate of Tran et al. protocol

In the above algorithm TT is the old transmission time of both RREQ and RREP packets at each node and computed as,

$$TT = \frac{RREQ_{Packetsize}}{Bandwidth} + \frac{RREP_{Packetsize}}{Bandwidth}.$$

5 Experimental results

This section describes the implementation of the proposed algorithm and analyses the results of the experiments. The proposed algorithm is simulated with NS3 with the parameters listed in Table 1. We analyse the simulation results based on the calculation of RTT in conjunction with processing time. The results of the proposed method have been compared with Tran et al. protocol [24].

5.1 Performance analysis

To evaluate the effectiveness of our proposed protocol, we consider four different scenarios for WMNs with 10 nodes, 20 nodes, 40 nodes and 60 nodes in the presence of a wormhole attack. Our proposed protocol identifies the malicious link by comparing the difference between old RTT and new RTT along the route. We have considered a threshold value (μ) to 100 ms under the consideration of processing time. If the value obtained after comparison is more than the threshold value then it confirms that the link between two nodes as wormhole link (Table 2).

From the simulation results, it is found that our proposed protocol with 40 nodes contains wormhole link between the two nodes in the network with RRT value 319.54 ms > 100 ms. As compared to our protocol we can see that Tran et al. protocol [24] detect wormhole link with 10 nodes and 40 nodes in the network, where the difference between the new RTT value and old RTT value is greater than a threshold value (i,e. 75.55 ms > 45 ms with 10 nodes and 319.54 ms > 45 ms with 40 nodes), this difference might be caused due to processing time which was not considered in Tran et al.'s protocol. However, according to our proposed protocol, it is proved that there is no wormhole attack in the network with 10 nodes (i.e. 75.55 ms < 100 ms) under the consideration of processing time. Detection rate is proportional to wormhole length, longer the wormhole link leads to more transmission delay between two malicious nodes. Threshold value is selected to compute the false positive rate and false negative rate with different wormhole length. False positive rate means higher rate of wrong detection and false negative rate means lower rate of wrong detection. Figure 6 shows that after fixed threshold value the false positive rate and false negative rate is almost similar to each other. Figure 7 shows that after fixed threshold value the false positive rate is much lower and false negative rate is much higher as compared to each other. Figure 8 shows the comparison of false positive rate between Tran et al. protocol and proposed protocol with different network size. Figure 9 shows the comparison of false negative rate between Tran et al. protocol and proposed protocol with different network size. Based on Figs. 8 and 9, the detection rate under different wormhole length with 10 nodes, 20 nodes, 40 nodes and 60

Table 2 Simulation results

	Old RTT (ms)	New RTT (ms)	New RTT − old RTT (ms)
With 10 nodes	253.52	329.07	75.55
With 20 nodes	36.27	36.37	0.1
With 40 nodes	256.77	576.31	319.54
With 60 nodes	177.01	211.32	34.31

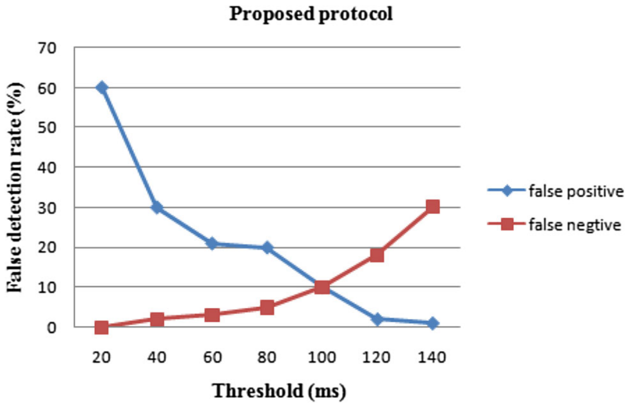


Fig. 7 False detection rate of proposed protocol

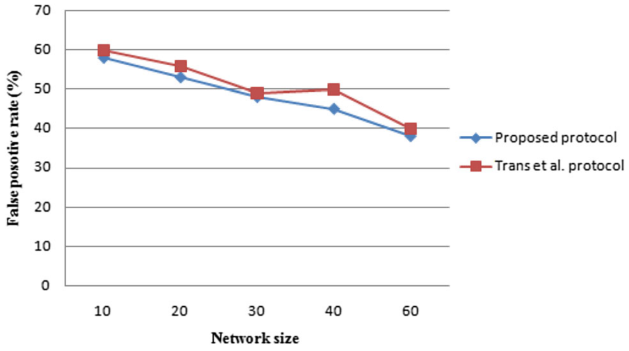


Fig. 8 False positive rate comparison between Tran et al. protocol and proposed protocol

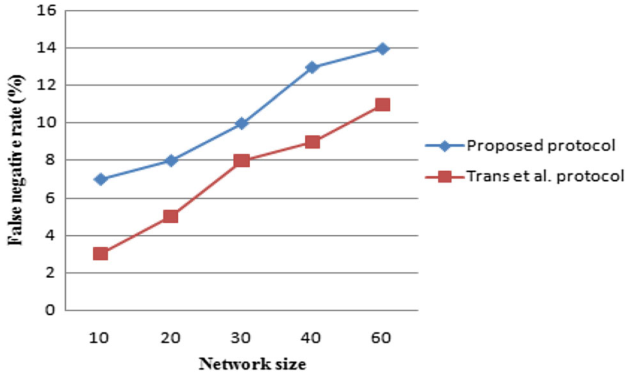


Fig. 9 False negative rate comparison between Tran et al. protocol and proposed protocol

nodes in the network is compared between proposed protocol and existing protocol shown in Fig. 10.

6 Conclusion

In this paper, we have proposed a RTT based algorithm in conjunction with processing time for the detection of malicious nodes in WMNs. Our proposed protocol achieves a higher detection rate of malicious nodes than the existing protocol in WMNs. The simulation is done in Network Simulator 3. Our experimental result is compared with the existing protocol and shows that the performance of the proposed protocol is better than the existing protocol. The comparison is mainly based on the detection rate. In future, the work could be further extended to achieve a more reliable and efficient detection protocol for WMNs by embedding new ideas to the proposed protocol.

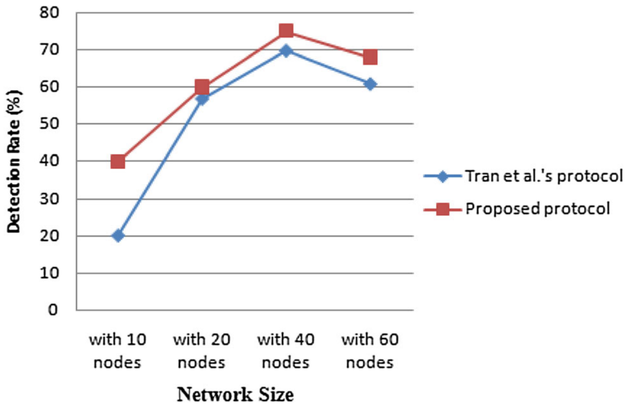


Fig. 10 Detection rate comparison between Tran et al. protocol and proposed protocol

Acknowledgements The authors of this paper would give full gratitude to the Computer Science and Engineering Department of Assam University for supporting the research to go in a smooth way. The research of this paper had carried out under the Department supervision along with the support of Departmental infrastructure.

References

1. Akyildiz IF, Wang X, Wang W (2005) Wireless mesh networks: a survey. Comput Netw 47(4):445–487
2. Kim J, Yun J, Yoon M, Cho K, Lee H, Han K (2010) A routing metric based on available bandwidth in wireless mesh networks. In: 2010 The 12th International Conference on Advanced Communication Technology (ICACT), IEEE, Phoenix Park, South Korea, ISBN: 978-1-4244-5428-0
3. Franklin AA, Murthy CSR (2007) An introduction to wireless mesh networks. In: Zhang Y et al (eds) Security in wireless mesh networks. CRC Press, Boca Raton
4. Sen J (2013) Security and privacy issues in wireless mesh networks: a survey. Wireless networks and security. Springer, Berlin, Heidelberg, pp 189–272
5. Khalil I, Bagchi S, Shroff NB (2005) LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. In: The international conference on dependable systems and networks (DSN). Pacifico Yokohama Conference Center, Yokohama, Japan, pp 612–621
6. Santhanam L, Xie B, Agrawal DP (2008) Selfishness in mesh networks: wired multihop MANETs. IEEE Wirel Commun 15(4):16–23
7. Altman Y, Keren AY (2016) U.S. Patent No. 9,479,523. Washington, DC: U.S. Patent and Trademark Office
8. Dromard J, Khatoun R, Khoukhi L (2013) A watchdog extension scheme considering packet loss for a reputation system in

wireless mesh network. In: 20th International Conference on Telecommunications (ICT 2013). Casablanca, Morocco, pp 1–5. http://www.ict-2013.org

9. Capkun S, Buttyán L, Hubaux JP (2003) SECTOR: secure tracking of node encounters in multi-hop wireless networks. In: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (in association with 10th ACM conference on computer and communications security). Fairfax, VA, United States
10. Dias JA, Rodrigues JJ, Xia F, Mavromoustakis CX (2015) A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks. IEEE Trans Ind Electron 62(12):7929–7937
11. Biswas J, Gupta A, Singh D (2014) WADP: a wormhole attack detection and prevention technique in MANET using modified AODV routing protocol. In: Arya KV, Sunil Kumar (eds) 9th international conference on industrial and information systems (ICIIS2014). IEEE, Piscataway, New Jersey
12. Liu X, Chen S, Song W (2014) A design and implementation of watchdog based on observer pattern and finite state machine. In: Proceedings of the 10th IEEE International Conference on Reliability, Maintainability and Safety (ICRMS '14), pp 407–411
13. Patel MM, Aggarwal A (2016) Two phase wormhole detection approach for dynamic wireless sensor networks. In: Proceedings of the IEEE international conference on wireless communications, signal processing and networking (WiSPNET '16). IEEE, Chennai, India. https://doi.org/10.1109/WiSPNET.2016.7566514
14. Su MY (2010) WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks. Comput Secur 29(2):208–224
15. Cho Y, Qu G, Wu Y (2012) Insider threats against trust mechanism with watchdog and defending approaches in wireless sensor networks. In: 2012 IEEE symposium on security and privacy workshops. IEEE, San Francisco, CA, USA. https://doi.org/10.1109/SPW.2012.32
16. Hernandez-Orallo E, Olmos MDS, Cano JC, Calafate CT, Manzoni P (2015) CoCoWa: a collaborative contact-based watchdog for detecting selfish nodes. IEEE Trans Mob Comput 14(6):1162–1175
17. Wang W, Bhargava B, Lu Y, Wu X (2006) Defending against wormhole attacks in mobile ad hoc networks. Wirel Commun Mobile Comput 6(4):483–503
18. Qian L, Song N, Li X (2007) Detection of wormhole attacks in multi-path routed wireless ad hoc networks: a statistical analysis approach. J Netw Comput Appl 30(1):308–330
19. Matam R (2013) Tripathy S (2013) WRSR: wormhole-resistant secure routing for wireless mesh networks. EURASIP J Wirel Commun Netw 1:180
20. Luan LY, Fu YF, Xiao P, Peng LX (2014) Preventing wormhole attacks in wireless mesh networks. In: Ma M, Qu X (eds) Applied mechanics and materials, vol 443, pp 440–445. https://doi.org/10.4028/www.scientific.net/AMM.443.440
21. Shamieh F, Refaey A, Wang X (2014) An adaptive compression technique based on real-time RTT feedback. In: 2014 IEEE 27th Canadian conference on electrical and computer engineering (CCECE). IEEE, Toronto, ON, Canada. https://doi.org/10.1109/CCECE.2014.6901082
22. Shams EA, Rizaner A (2018) A novel support vector machine based intrusion detection system for mobile ad hoc networks. Wirel Netw 24(5):1821–1829
23. Abdel-Azim M, Salah HED, Eissa ME (2018) IDS Against blackhole attack for MANET. Int J Netw Secur 20(3):585–592
24. Tran PV, Hung LX, Lee YK, Lee S, Lee H (2007) TTM: transmission time-based mechanism to detect wormhole attacks. In: 2007 4th IEEE consumer communications and networking conference. IEEE, Las Vegas, NV, USA. https://doi.org/10.1109/CCNC.2007.122