



Attacks Detection Based on Control Packets and Trust-Based Routing Protocol in MANET

Kavitha T¹, Dejeey²

Abstract

In a mobile ad-hoc network (MANET), a mobile node can forward data to other mobile node without any centralized services. Due to the lack of centralized services, some external attackers may attack the routing paths which established from source to destination. Among the attacks, wormhole, gray, and black hole attacks may misguide the routing messages between the nodes. So, this research work focuses to detect the wormhole, gray and black hole attacked paths between source and destination and also to select the most trusted routing path for data transmission. Thus, these attacked paths are detected based on the control packets Detection Packet (DeP) and Feedback Packet (FeP) among the 'M' paths which are generated using AOMDV protocol. Then, a trust-based routing protocol (TBRP) is presented where the trust score is calculated for each node using the optimized fuzzy system which was presented in our previous work. Depend on the trust of each node, the most trust route is estimated. Simulation results depict the TBRP protocol performs better than the existing routing protocol DSR and TDSR in terms of throughput and delivery ratio.

Key Words: MANET, Attack Detection, Control Packets, Trust-Based Routing Protocol (TBRP), Optimized Fuzzy System.

DOI Number: 10.14704/nq.2022.20.8.NQ44228

NeuroQuantology 2022 ;20(8):2094-2105

Introduction

In MANETs, attacks by and large reason and they are first isn't to forward the data packet or modify the parameters of routing messages and to deplete the battery of nodes by make them navigating some fake packet in the misguided path and they likewise modify the parameters of the packets, for example, sequence numbers and by utilizing scheme like cryptography or authentication as a preventive scheme and can be utilized against attackers [1-4]. Using these schemes, attacks from outside can be prevented yet not from any node inside by utilizing this data can take risks in the network. This may prompt false positive detection of a

from devouring their resources, for example, battery, by not taking an interest in the operations of the network. Subsequently, selfish nodes additionally influence the performance of the network as they don't accurately deal with network packets, for example, in routing schemes [5] [6]. The major security danger to routing is the chance of third party disturbing traffic by weakening the routing schemes. The conveyance of bogus routing data permits the capability of accidental routing loops of the network, wormhole, gray and black hole attacks, or other non-practical routes [7-9]. These attacks may ruin or disallow the communication essential to satisfying the mission of network nodes.

non-malevolent node. Selfish nodes abstain

Corresponding author: Kavitha T

Address: ¹Assistant Professor, Department of CSE, AU Regional Centre– Tirunelveli, Tamil Nadu, India; ²Assistant Professor, Department of CSE, AU Regional Centre – Tirunelveli, Tamil Nadu, India;

³E-mail: tkavitha2022@gmail.com

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Received: 13 March 2022 **Accepted:** 18 April 2022



It is consequently basic for nodes to progressively decide the legitimacy of routing data preceding settling on routing decisions. With encryption and authentication schemes, secure routing protocols have been designed to guarantee properties, for example, integrity and confidentiality. These protocols need a centralized trusted third party, which is unfeasible for MANETs. Additionally, the conventional cryptosystem depends security scheme is regularly used to oppose external attacks. So, the following contributions are presented in this paper.

- From source to destination 'M' multipaths are generated using AOMDV protocol.
- By verifying the control packets DeP and FeP, the source node detects the wormhole, gray and black hole attacked paths
- After identifying the attacked paths, the trust score of every node is calculated using the optimized fuzzy system.
- Depend on the trust score of intermediate nodes, the trust of the routing path is estimated using the proposed TBRP.

The remaining sections of the paper are sorted as pursues. Section 2 relates few recent articles that presented research on attack detection and routing in MANET. Section 3 proposes control packets based on the wormhole, gray, and black hole attacks detection and TBRP. Section 4 analyses the results of TBRP. Conclusion of the work is described in section 5.

Related works

The nodes in MANET communicate with one another through a remote correspondence medium and make this network profoundly defenseless against numerous attacks. One of the notable attacks is the packet drop attack. At whatever point the network faces any sort of attack unexpectedly decreases the performance of the network. So, Premala Bhande and MD. Bakhar [10] had developed a protocol called swarm intelligence based cross-layer packet drop attack detection abbreviated as CLPDM-SI. This scheme pursued a collective swarm intelligence detection scheme based on the cluster to discover a malicious node in a genuine data securing framework which goes through a packet drop attack. The comparison was made dependent on different QoS parameters such as delivery ratio, delay, and throughput. By investigating memory utilization and CPU processing time, the calculation found the false

positive of malicious nodes.

In comprehensive conditions, a few nodes don't help out different nodes in identifying the efficient route to the destination and purposefully pass the information of false route of containing the shortest path to the destination and start packet dropping as opposed to sending it. This kind of misbehaviour is commonly known as a black hole attack. So, Shashi Gurung and Siddhartha Chauhan [11] had presented a protocol known as Mitigating Black Hole impacts via Detection and Prevention abbreviated as MBDEP-AODV. By presenting this proposed scheme, the author attained maximum throughput and delivery ratio.

The black hole attack primarily bothers the data collection and takes an attempt to take part in the majority of the connections as conceivable to expand the resource-restricted problems in the network. To solve these problems, R. Tino Merlin and R. Ravi [12] had presented a new energy-aware routing based on trust abbreviated as TEAR for MANETs. The TEAR system mitigated black holes via the multiple routes and identified the black holes rapidly as could be expected under the circumstances and gave better security of data routes by attaining the trust of a node. The simulation results of the article depict that the TEAR increased the successful data routing probability.

A Cooperative black hole is created by at least two attackers with common handshaking. The nodes act regularly in equal communication and interaction. Kapil Juneja [13] had proposed the suspected node assessment model based on a session to recognize and remove the cooperative blackhole attacks. A session was set up for the evaluation of earlier communication as the communication starts. The parameter explicit assessment was executed over the session to distinguish the suspected nodes. After the completion of the session, the continuous monitoring of suspected nodes' behavior was performed all through the communication. Besides, the K-neighbour assessment technique was applied to perceive the suspected nodes' cooperative attack. The assessment was performed arbitrarily on more modest separate sessions during the



correspondence. The notice on nodes was likewise done based on perceiving the safe or attacker node. The conjunctive connection degree in a stream is monitored to perceive the cooperative attacker nodes. Because of this proposed scheme, the authors had increased the packet delivery ratio.

The connection between the nodes can be disappeared at any time due to the dynamic topology of MANET. This type of characteristic leads the network to affect by the attacks. Among the various attacks, the wormhole attack forwards the fake shortest path message to the destination having the aim of corrupting the communication. So, Ashish Kumar Jain and Jyoti Patidar [14] had presented a novel wormhole detection scheme. In the simulation, the authors had considered the parameters such as count of packet drop, throughput, and delay. Besides, they had presented an interchange for routing to prevent the network. Because of the proposed approach, the authors had achieved a better throughput.

The Wormhole attack performs in two different ways. Initially, the genuine nodes are convinced by the malicious nodes for transmitting the data via them to interfere in more routes. Second, malicious nodes extract data in different ways. So, Farrukh Aslam Khan et al [15] had presented a DEPS system for recognizing and removing the malicious nodes. In the proposed scheme, few special nodes were utilized that known as DEPS nodes. These nodes were used to monitor the other nodes' behavior. If the nodes had found the behavior of malicious nodes, it finalized that the node was a wormhole node by transmitting a message. Finally, the network canceled whole data and control messages from the wormhole node. Because of the proposed scheme, packet drop, as well as the rate of false-positive, was decreased.

Shashi Gurung and Siddhartha Chauhan [16] had proposed a novel scheme for alleviating the effect of a smart gray hole attack. The proposed Mitigating Gray hole Attack Mechanism abbreviated as MGAM utilized a few exceptional nodes known as gray hole-IDS abbreviated as G-IDS which were performed for

identifying and removing smart gray hole attack. These nodes monitored the transmission of its neighbouring nodes and when it recognized that the node was losing the data which were more noteworthy than the threshold value then it forwards the ALERT message telling about the malicious node's activity. Because of this proposed scheme, the authors had achieved a better delivery ratio and throughput.

To enhance the network security, Zhiping Jia et al [17] had proposed a dynamic trust prediction framework in MANET. Based on the historical behaviors and future behaviors of the nodes, nodes' trustworthiness was calculated using the extended fuzzy logic rules prediction. Besides, the authors had enhanced the prediction framework to secure the routing scheme. The proposed unicast routing protocol based on on-demand trust also known as Source Routing protocol based on trust abbreviated as TSR offered a feasible and flexible to select the shortest path that solved the security issue in the transmission of data packets.

Attacks Detection Based on Control Packets and Trust-Based Routing In MANET

1. Overview

Figure 1 illustrates the flow diagram of the approach. Initially, from source to destination, 'M' paths are generated utilizing AOMDV. Next, the source node detects the wormhole, gray, and black hole attacks attacked routes by checking the DeP and FeP from the destination. After the detection of attacks in the routing path, the attacked or malicious nodes are ignored from the paths. Then, before transmitting the data packet, the most trustable routing path is to be selected. So, the trust score of each node is calculated using the optimized fuzzy system was presented in our previous work. Depend on the trust score of intermediate nodes, the trust value for a route is calculated. After calculating the trust value of each route, the source node chooses the route which having the highest value of trust.



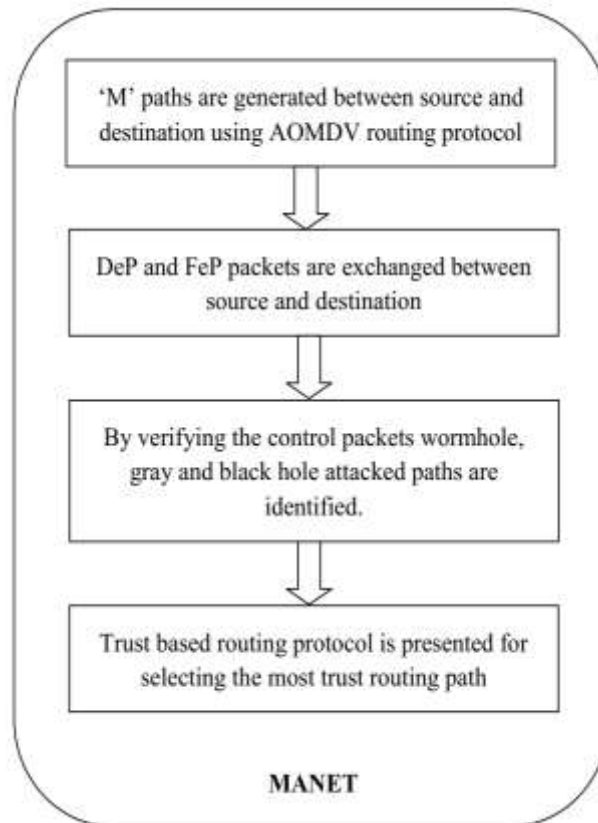


Fig. 1. Flow diagram of the proposed protocol

2. AOMDV Routing Protocol-Based M-Paths Generation

At first, multiple paths are established between source (n_s) and destination (n_d) in MANET. For the establishment of multiple paths, the AOMDV is utilized in this

methodology. Employing AOMDV, the source node forwards RREQ (route request) to its nearby nodes, and the nodes structure a route to the destination if they have a path in the RT (routing table). The destination node forwards the RREPs (route replies) to the source node after receiving the RREQs. Then through these multiple paths, n_s starts to forward the data to the destination.

3. Attacks Detection Based on Control Packets

Because of some intermediate nodes, fake routing messages might be generated and forwarded in the routing paths. These routing messages misguide the neighbor nodes that the routing path is shorter than the original path. This kind of attacked path is called a wormhole attacked path. Besides, some other kind of intermediate nodes may drop packets or control all received data packets. This kind of attacked path is called a gray and black hole attacked path. So, before forwarding the data packets through the established 'M' paths, the source node needs to

detect whether a routing path is attacked by the attackers or not. Thus, for detecting the wormhole, gray and black hole attacked paths among the 'M' paths, the control packets Detection Packet (DeP) and Feedback packet (FeP) are used in this approach.

Initially, the n_s forwards the DeP to n_d via the intermediate nodes. Figure 2 illustrates the DeP structure. This DeP packet consists of the information of source ID (SID), round trip time (RTT), hop-count, sending sequence (SSeq), and destination ID (DID). Here, hop-count defines the count of intermediate nodes performing in a routing path. Source ID denotes the source node's identity, as well as DID, represents the identity of n_d . The sending sequence represents the update of the route from the source. For m^{th} route, RTT is determined depend on the receiving time of RREQ (T_r) and the transmitting time of RREQ (T_t). It can be defined as follows:

$$RTT_m = T_r - T_t \tag{1}$$

Besides, by computing the average RTT of available routing paths, threshold Round Trip Time (RTT_{th}) is determined.

Then the n_d sends the FeP packet to the n_s via the same routing path once it receives the DeP packet. The structure of FeP is shown in figure 3. As shown in



the figure, the structure of FeP consists of DID, RTT, hop-count (HC), destination sequence (Dseq), and SID. Here, the destination sequence represents the update of the route from the n_d . After getting the FeP packet, the source node initiates to verify the packets

Source ID	RTT	Hop-Count	SSeq	Destination ID
-----------	-----	-----------	------	----------------

Fig. 2. DePStructure

Destination ID	RTT	Hop-Count	Dseq	Source ID
----------------	-----	-----------	------	-----------

Fig. 3. FeP Structure

Wormhole attack detection

- After getting the FeP, the source node verifies the information hop-Count and RTT_m of DeP
- The source node matches the RTT_{th} with the RTT_m of every path. The route is considered as a malicious path which is attacked by wormhole when the RTT_m is less than the RTT_{th} and the HC of the routing path is equals to the threshold HC 2.
- Else, the routing path is detected as normal path.

Gray and black hole attacks detection

- Every intermediate node forwards the Sseq to the neighbor nodes. After receiving Sseq, the neighbor node forwards the response sequence (Rseq) to the corresponding intermediate node.
- Through this way, information on the route is updated in each intermediate node. Finally, n_a gets the Sseq and transmits the Dseq to n_s via the same path.
- After receiving the Dseq, n_s matches the Dseq and Sseq. If the Dseq is greater than the Sseq, then the corresponding path is considered as the gray and black hole attacked path.

Algorithm 1: Detection of Wormhole, Gray and Blackhole attacked paths

1. Generate 'M' paths using AOMDV between the source and destination.

for identifying the attacked paths among the 'M' paths between the source and destination.

2. n_s forwards the DeP packet to n_d before initiating the transmission of the data packet.
3. n_d forwards FeP packet to n_s after receiving DeP.
4. After receiving FeP, the source node verifies the information of DeP and FeP packets.

Malicious node detection

5. If $hop-count_m = 2$ and $RTT_m < RTT_{th}$
- Then

The source node decides that the m th Path is a wormhole attacked path

6. Else
- The source node decides that the m th Path is an attack free path.

7. End

Gray and black hole attacks detection

8. If $DSeq_m > SSeq_m$
- Then

The source node decides that the m th Path is a gray and black hole attacked path

9. Else

The source node decides that the m th Path is an attack free path.

10. End



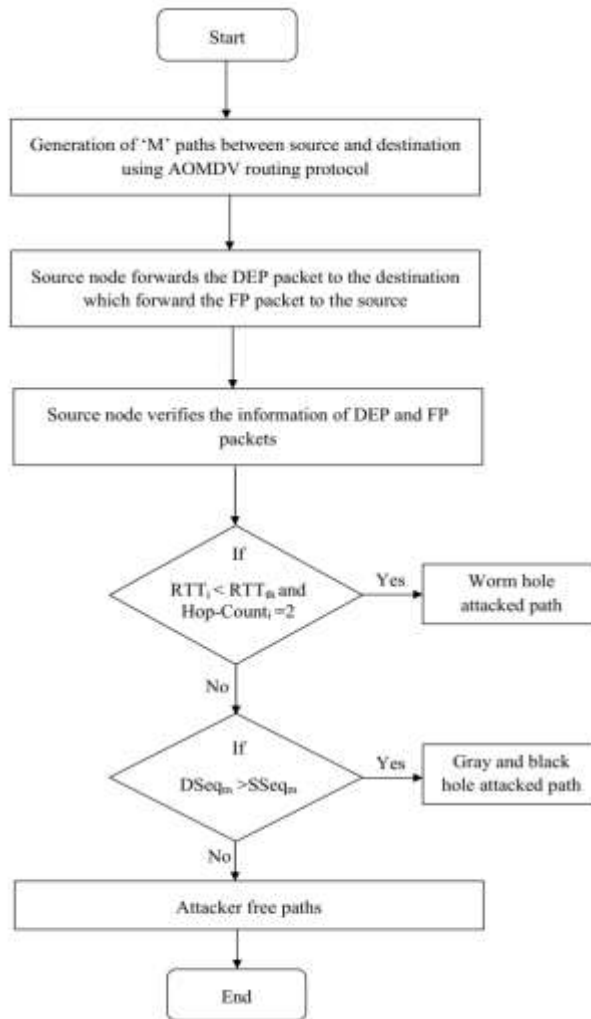


Figure 4: Flow chart of the attack detection

4. Trust-based routing protocol (TBRP)

After the detection of attacks, the attacked or malicious nodes are ignored from the paths. Then, before transmitting the data packet, the most trustable routing path is to be selected. So, the trust score is calculated for each node using the optimized fuzzy system was presented in [18]. A short explanation of the trust score calculation is given as follows:

Depend on the trust score of intermediate nodes, the trust value for a route is calculated using equation (2).

Depend on the trust score of intermediate nodes, the trust value for a route is calculated using equation (2).

$$T_{Route}(t) = \prod \left(\left\{ T_i(t) \mid n_s \rightarrow n_d / Route(R) \right\} \right) \quad (2)$$

Where, n_s and n_d denote the source and destination node respectively and $T_i(t)$ denotes the trust score of the i^{th} node in the route R . If n_d is a neighbour of n_s , the trust of the path is considered as 1 as all packets sent in one hop will reach the desired neighbor (node n_d). After calculating the trust of each route, the n_s chooses the route which having the highest trust value. At final, the n_s transmits the data to n_s via the chosen routing path. Figure 5 shows an example of the trust route selection between n_s and n_d . As shown in the figure, the different paths between n_s and n_d are P1 (n_s, n_1, n_2, n_d), P2 (n_s, n_3, n_4, n_d), and P3 (n_s, n_3, n_2, n_d). Also, trust of intermediate nodes n_1, n_2, n_3 and n_4 are valued as 0.8, 0.92, 0.83 and 0.98 respectively. According to equation (2), trust for three paths is calculated and valued as $T(P1) = 0.73$, $T(P2) = 0.81$ and $T(P3) = 0.76$. Among the three paths,



$P2 (n_s, n_3, n_4, n_d)$ is selected as the most trusted path.

The calculation of route trust considers trust estimations of every single intermediate node. The trust of the route means a joint likelihood at which data will be sent if they are forwarded via the routing path. The trust of a route is the trust experienced by the previous packet which has shown up along the course.

Since network load situations will alter every once in a while during the communication, the trust will likewise change in like manner. By utilizing the most recent showed up data packet to ascertain Route $T_p (t)$, the method is versatile to changing conditions of the network and the source will be accurately informed conveniently for a 'Handoff' so the loss of packet can be limited.

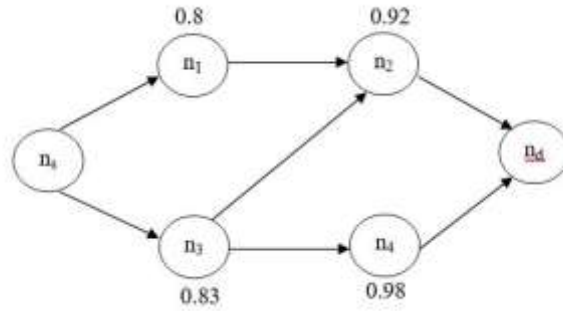


Fig. 5. The example of the trust route selection between n_s and n_d .

Results and Discussion

The proposed approach of this research work is simulated in the NS2. Table 1 illustrates the simulation setting of the proposed approaches. As shown in the table, 250 mobile nodes are deployed in the size of 1000m X 1000m simulation area. Moreover, Besides in this simulation, CBR and 802.11 MAC standard are used in this simulation. Simulation time for each approach is 200 secs.

Table 1. Simulation setting

Parameters	Assumptions
Area	1000m X 1000m
Number of Nodes	250
Rate	500Kbps
MAC	802.11
Simulation time	200secs
Traffic Source	CBR
Antenna	Omni antenna
Propagation	TwoRayGround
Routing protocol	AOMDV
Packet size	512 byte



1. Performance analysis

The execution of the TBRP is evaluated and compared with that of the traditional routing protocols DSR and TDSR based on the number of attackers and speed of the mobile nodes.

The performance analysis depend on the number of attackers

The performance of the different routing protocols such as TBRP, TDSR, and DSR is evaluated. Figure 6 illustrates the comparison of delay of the different approaches for a varying number of attackers. As shown in the figure, compared to TDSR and DSR, the delay of the TBRP is reduced to 46% and 61% respectively. Comparison among TBRP, TDSR, and DSR in terms of the delivery ratio is shown in figure 7. As the TBRP is presented with the AOMDV routing protocol, the calculation of route trust is simplified than TDSR as well as DSR. So, it enhances the secure data transmission through the trust route and also it improves the delivery

ratio of the network. Namely, the delivery ratio of the TBRP is increased to 13% and 78% than that of TDSR and DSR respectively. Figure 8 illustrates the network lifetime of different approaches. As the wormhole, gray and black hole attacked paths are identified and ignored using the control packets, the network lifetime of the network is improved. Namely, as shown in the figure, compared to TDSR and DSR, the network lifetime of the TBRP is increased to 50% and 82% respectively. The comparison of the throughput of the different routing protocols is depicted in figure 9. Due to the proposed TBRP with AOMDV routing protocol, the throughput of the network is increased to 13% and 35% than the existing routing protocols TDSR and DSR respectively. Figure 10 illustrates the comparison of energy consumption of different protocols. As shown in the figure, compared to TDSR and DSR, the energy consumption of TBRP is reduced to 29% and 48% respectively.

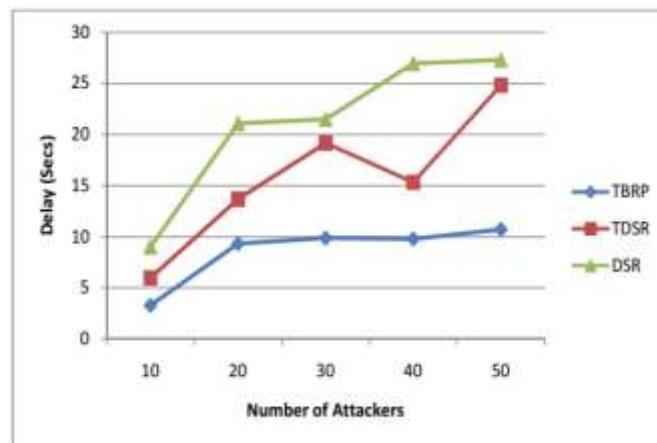


Fig. 6. Comparison of delay of routing protocols for varying attackers

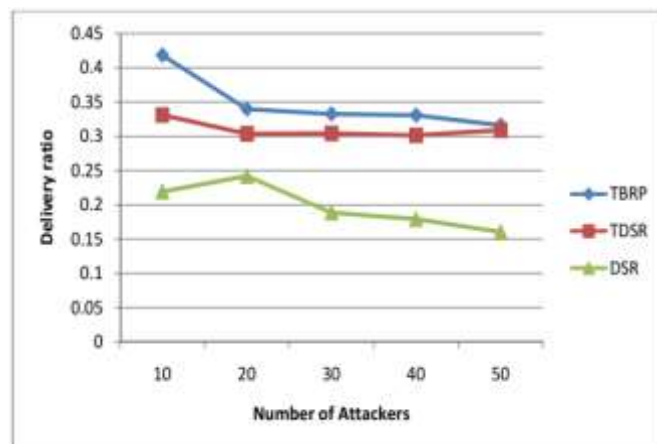


Fig. 7. Comparison of delivery ratio of routing protocols for varying attackers



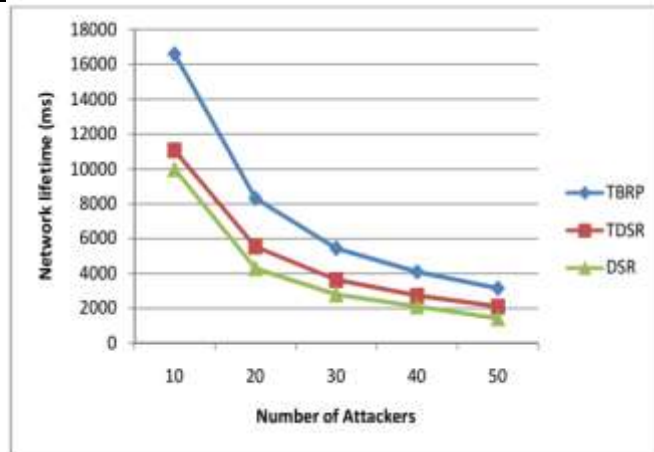


Fig. 8. Comparison of network lifetime of routing protocols for varying attackers

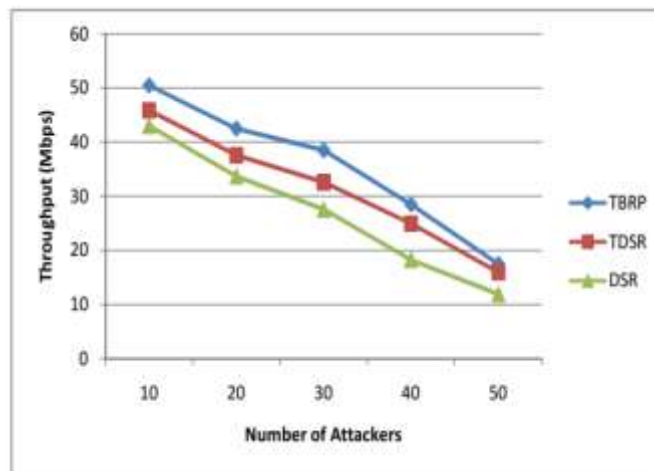


Fig. 9 Comparison of throughput of routing protocols for varying attackers

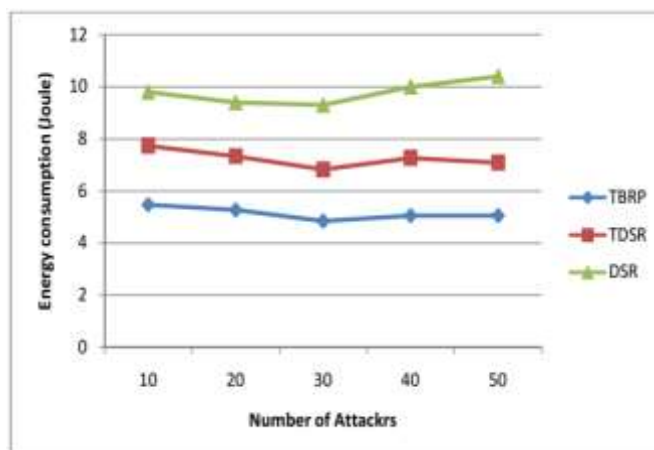


Fig. 10. Comparison of energy consumption of routing protocols for varying attackers

The performance analysis depend on the speed of the nodes

The performance of the different routing protocols such as TBRP, TDSR, and DSR is evaluated for varying speed of mobile nodes.

Figure 11 shows the comparison among TBRP, TDSR, and DSR in terms of delivery ratio. The delivery ratio of the TBRP is increased to 32% and 54% than that of TDSR and DSR respectively. Figure 12 illustrates the comparison of energy consumption of different



protocols for varying speed of mobile nodes. Compared to TDSR and DSR, the energy consumption of TBRP is reduced to 22% and 34% respectively. Figure 13 illustrates the comparison of delay of the different approaches. Compared to TDSR and DSR, the delay of the TBRP is reduced to 19% and 37% respectively. Figure 14 illustrates the network lifetime of different approaches. As shown in

the figure, compared to TDSR and DSR, the network lifetime of the TBRP is increased to 34% and 86% respectively. The comparison of the throughput of the different routing protocols is depicted in figure 15. Due to the proposed TBRP with AOMDV routing protocol, the throughput of the network is increased to 23% and 70% than the existing routing protocols TDSR and DSR respectively.

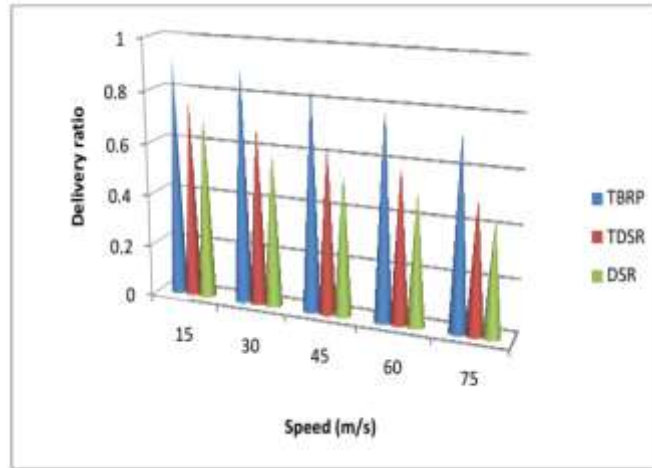


Fig. 11. Comparison of delivery ratio of routing protocols for varying speed

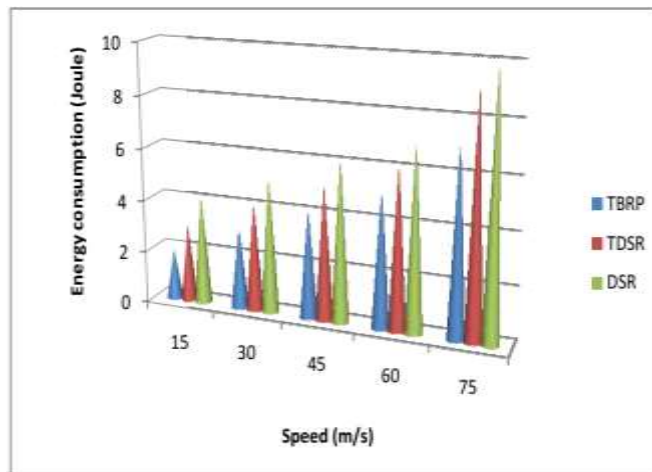


Fig. 12. Comparison of energy consumption of routing protocols for varying speed

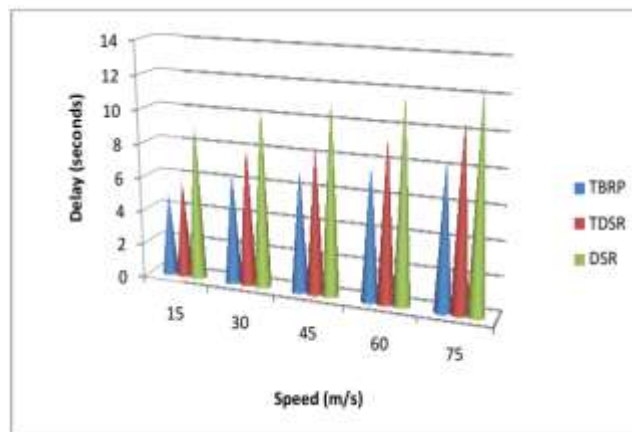


Fig. 13. Comparison of delay of routing protocols for varying speed



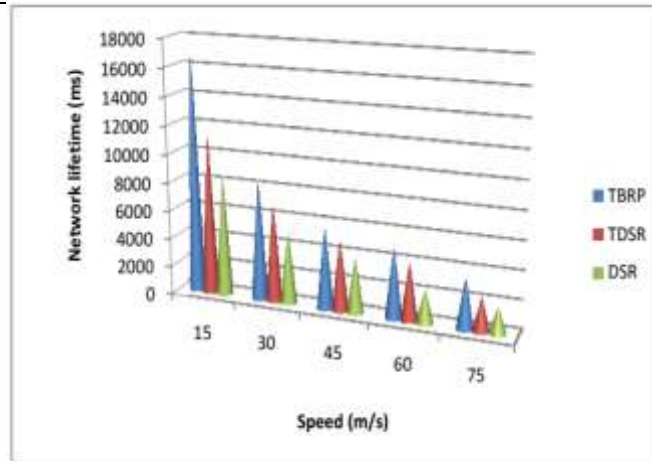


Fig. 14: Comparison of network lifetime of routing protocols for varying speed

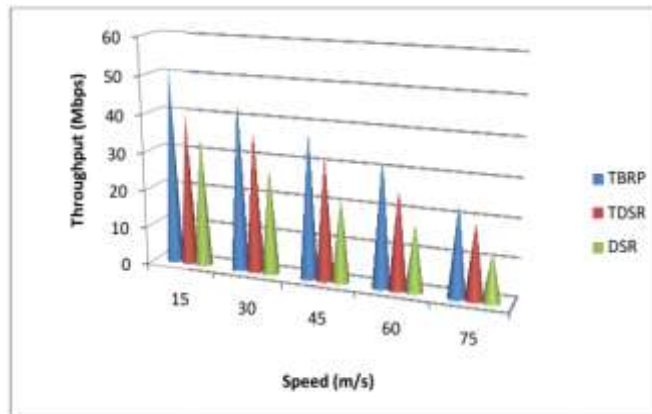


Fig. 15: Comparison of throughput of routing protocols for varying speed

Conclusion

To enhance the security against attackers in the MANET, control packets based attack detection and trust-based routing protocol (TBRP) has been presented in this paper. Initially, between the source and destination, ‘M’ paths have been generated using the AOMDV routing protocol. Then, based on the control packets Detection Packet (DeP) and Feedback Packet (FeP), the source node has detected the wormhole, gray and black hole attacked paths. After the detection of attacked paths, a trust score has been calculated for each intermediate node in the attack-free path using an optimized fuzzy system. Depend on the trust score of each node, the trust route is calculated. The performance of the TBRP is evaluated for a varying number of attackers and mobile nodes. Also, compared to DSR and TDSR, the proposed TBRP achieves better throughput and delivery ratio.

Acknowledgment

The authors appreciate the assistance of the

University of Technology's Applied Science Department, Kerbala University's Physics and Chemistry Departments, and University of Babylon, in completing this project.

Conflict of Interest

The authors confirm that this manuscript content has no conflict of interest.

References

Gawande, Prachi D., and Yogesh Suryavanshi. "Cryptography based secured advanced on demand routing protocol in MANET's." In 2015 International Conference on Communications and Signal Processing (ICCSP), pp. 1478-1481. IEEE, 2015.

Zhao, Shushan, Akshai Aggarwal, Richard Frost, and Xiaole Bai. "A survey of applications of identity-based cryptography in mobile ad-hoc networks." IEEE Communications Surveys & Tutorials 14, no. 2 (2011): 380-400.

Guan, Quansheng, F. Richard Yu, Shengming Jiang, and Victor CM Leung. "Joint topology



control and authentication design in mobile ad hoc networks with cooperative communications." *IEEE Transactions on vehicular technology* 61, no. 6 (2012): 2674-2685.

Bu, Shengrong, F. Richard Yu, Xiaoping P. Liu, and Helen Tang. "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks." *IEEE Transactions on Wireless Communications* 10, no. 9 (2011): 3064-3073.

Ramya, N., and S. Rathi. "Detection of selfish Nodes in MANET-a survey." In 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS), vol. 1, pp. 1-6. IEEE, 2016.

Xu, Li, Zhiwei Lin, and Ayong Ye. "Analysis and countermeasure of selfish node problem in mobile ad hoc network." In 2006 10th International Conference on Computer Supported Cooperative Work in Design, pp. 1-4. IEEE, 2006.

Sharma, Pawan Kumar, and Vishnu Sharma. "Survey on security issues in MANET: Wormhole detection and prevention." In 2016 International Conference on Computing, Communication and Automation (ICCCA), pp. 637-640. IEEE, 2016.

Roshani, Parmar, and Ankit Patel. "Technique to mitigate grayhole attack in MANET: A survey." In 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1-4. IEEE, 2017.

Sarma, Kishor Jyoti, Rupam Sharma, and Rajdeep Das. "A survey of black hole attack detection in manet." In 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 202-205. IEEE, 2014.

Bhande, Premala, and M. D. Bakhar. "Cross layer packet drop attack detection in MANET using swarm intelligence." *International Journal of Information Technology* (2019): 1-10.

Gurung, Shashi, and Siddhartha Chauhan. "A dynamic threshold based approach for mitigating black-hole attack in MANET." *Wireless Networks* 24, no. 8 (2018): 2957-2971.

Merlin, R. Tino, and R. Ravi. "Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET." *Wireless Personal Communications* 104, no. 4 (2019): 1599-1636.

Juneja, Kapil. "Random-session and K-neighbour

based suspected node analysis approach for cooperative blackhole detection in MANET." *Wireless Personal Communications* 110, no. 1 (2020): 45-68.

Jain, Ashish Kumar, and Jyoti Patidar. "Detecting Packet Dropping Misbehaving Nodes in MANET Using RTT." In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), pp. 1323-1328. IEEE, 2018.

Khan, Farrukh Aslam, Muhammad Imran, Haider Abbas, and Muhammad Hanif Durad. "A detection and prevention system against collaborative attacks in mobile ad hoc networks." *Future Generation Computer Systems* 68 (2017): 416-427.

Gurung, Shashi, and Siddhartha Chauhan. "A novel approach for mitigating gray hole attack in MANET." *Wireless Networks* 24, no. 2 (2018): 565-579.

Xia, Hui, Zhiping Jia, Xin Li, Lei Ju, and Edwin H-M. Sha. "Trust prediction and trust-based source routing in mobile ad hoc networks." *Ad Hoc Networks* 11, no. 7 (2013): 2096-2114.

Thangaraj, K. and Dharma, D., 2020. Optimized Fuzzy System Dependent Trust Score for Mobile AdHoc Network. *Wireless Personal Communications*.

