JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 35, 805-820 (2019)
DOI: 10.6688/JISE.201907_35(4).0006

A Secure Link Aware Fault Detection Algorithm for Enabling a Reliable Communication in MANET

K. GOKILA[1,*] AND ILA. VENNILA[2]
[1]*Department of Electronics and Communications Engineering*
[2]*Department of Electrical and Electronics Engineering*
PSG College of Technology
Tamil Nadu, 641004 India

Providing a secure communication in Mobile Ad-hoc Network (MANET) is one of the demanding and critical task in recent days, due to its dynamic nature. So, the traditional works focused to develop a secure routing protocols for detecting the harmful attacks in network. But, it failed to ensure the fault free link during communication, which affects the entire performance of the network. Also, it follows a single stage attack detection process, in which the attacks are detected at before routing or during data communication. So, the detection accuracy of the existing techniques is not highly efficient. Thus, this work motives to introduce a new routing mechanism, namely, Secure Link Aware Fault Detection (SLFD) for enabling a secure and fault free data communication in MANET. At first, the neighbor discovery and route discovery processes are performed by sending the HELLO packets and RREQ to the neighboring nodes that are in the range of < 200m. After that, the attack detection process is performed by analyzing the behavior of the malicious nodes. In this environment, two harmful attacks such as black hole and gray hole are detected and blocked before communication. Then, the route between the trusted nodes are enabled by analyzing the link paths with the use Genetic Algorithm (GA). Furthermore, the data is transmitted by generating the bogus key and validating the authenticity of the nodes. During this process, the Jitter is also estimated for identifying the compromised nodes in the route. During simulation, the effectiveness of the proposed system is analyzed and validated by using different performance measures. Also, the superiority of the SLFD is proved by comparing it with the existing approaches.

Keywords: mobile ad-hoc network (MANET), secure link aware fault detection (SLFD), black hole attack, gray hole attack, link stability analysis, genetic algorithm, jitter calculation

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a self-organized network that contains a set of wireless nodes for communication [1]. In this environment, the communication between the nodes are performed based on the bandwidth constrained links [2]. The major characteristics [3, 4] of MANET are as follows: autonomous, multi-hop routing, band width optimization, physical security, and no fixed infrastructure. Due to these reasons, it is widely in many application areas [5] such as military, battlefields, fire detection, and other emergency applications. So, providing security to this network is highly imperative and critical in these days. Also, the links stability [6, 7] is must be considered in order to ensure the successful data transmission. Moreover, the data in the form of video streams are highly difficult to transmit, because it requires a stable path during communication

Received December 30, 2017; revised January 9, 2019; accepted March 10, 2019.
Communicated by Ralf Klasing.

[8]. The general architecture of MANET is shown in Fig. 1. Attack identification and detection is also an imperative task in MANET, because it reduces the overall performance of the network. There are different types of attacks [9, 10] that present for reducing the QoS of MANET. So, the network must be protected against the attacks by implementing an efficient security mechanism.

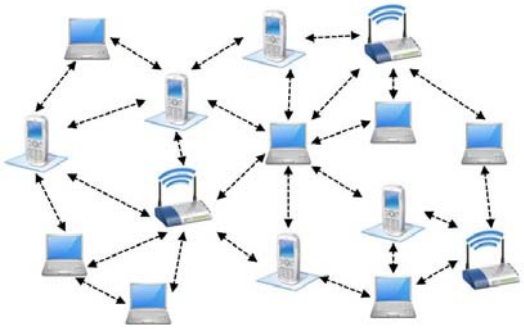

Fig. 1. Architecture of MANET.

A. Problem Identification

Due to the broadcasting nature of MANET, the packet redundancy and broadcast storm problems can be occurred. Typically, the traditional works developed some approaches based on Network Coding (NC) for addressing this problem, which integrates many packets in one coded packet for improving the transmission performance [11]. But, it has the major problems of reduced delivery rate, throughput, increased energy loss, data dropping, and retransmission rate [12, 13]. In our previous work [14], the network stability is concentrated by calculating the link quality measures. But, it does not satisfy the user requirements in terms of video transmission, because the data communication adjusts the data rates by finding the best link between the source and intermediate nodes. So, it does not support the data, if it is in the form stream (*i.e.* audio or video). Moreover, the external security based problems are not focused in our previous work. To solve these issues, this research work aims to develop a new security mechanism by considering the measures of both link stability, and attack detection.

B. Objectives

The major research objectives of this paper are as follows:

- To securely transmit the data in the network, a Secure Link aware Fault Detection (SLFD) mechanism is proposed.
- To analyze the link for detecting the failures, a Genetic Algorithm (GA) is utilized that checks the stability of the links during data transmission.
- To enable an error free communication, a bogus key generation and node authentication processes are performed.
- To identify the compromised nodes in the route, a Jitter is calculated between the pair of nodes.

C. Organization

The rest of the sections that structured in the paper are as follows: the existing routing mechanisms and security approaches used for MANET security are investigated in Section 2. The detailed description about the proposed methodology with its clear flow has been represented in Section 3. The simulation results of both existing and proposed mechanisms are validated with respect to different measures in Section 4. Finally, the overall paper is concluded and the future enhancement that can be implemented in the next phase are stated in Section 5.

2. RELATED WORKS

In this sector, the existing algorithms that used for link stability analysis and secure routing in MANET are surveyed with its advantages and disadvantages.

Rhaiem *et al*., [15] implemented a network coding mechanism for improving the quality of videos during video streaming in MANET. Here, the cross layer approach was developed to reduce the end-to-end delay with the use of Multicast Scalable Video Transmission using Classification Scheduling Algorithms and Network Coding (MSVT_CSA _NC) technique. Here, an efficient video streaming was enabled based on the temporal, spatial, and quality properties. Before transmission, the priority of the packets was analyzed by choosing the appropriate block size. Kumar [16] aimed to detect the Jelly Fish (JF) attack during video streaming by implementing the delay variance attack. The major objectives that focused in this work were to reduce the delay and increase throughput. In this paper, the authors stated that a monitoring mechanism was required to identify and isolate the attacks in network. Castellanos *et al*., [17] suggested a QoS routing protocol for detecting the link failures in the route by analyzing the bandwidth usage. Here, the route recovery mechanism was implemented for re-establishing the connection between the nodes. In this work, the same video was integrated with a same bit stream by using a scalable video coding technique. Also, the cross layer approach was utilized to estimate the available bandwidth in the network. Moreover, the intra-flow contention was calculated by using the measure of contention count.

Malathi and Jayashri [18] developed a new routing protocol for minimizing the path delay and ensuring the reliable communication in the network. Also, a Power Proficient Reliable Routing (P2R2) protocol was utilized by enabling an error free path with increased energy, channel quality, and link quality. The major advantages of this work were increased QoS, reduced packet loss ratio, and overhead. However, it required to improve the efficiency of routing by avoiding the congestion in the network. Saeed, *et al*., [19] developed a unique localization algorithm for reducing the energy consumption of the network. In this work, the active approach was utilized to provide a better solution for solving the energy cost problem. Also, the duty cycles of the sensor nodes in the network were controlled with reduced energy consumption by analyzing the Time of Arrival (TOA). The drawback that observed from this work was it required to prove the effectiveness of the suggested work by evaluating different measures. Rafsanjani and Fatemidokht [20] designed a fuzzy logic based routing protocol for analyzing the security threats in MANET. Here, the digital signature was utilized to validate the integrity of the node and the fuzzy set theory was employed to estimate the trust value of the node.

The major focuses of this work were to reduce the delay, increase the throughput, and transmission efficiency. But, this work failed to detect the selfish nodes in the network, so the security of the network was affected. Usha *et al*., [21] utilized a cross layer security approach, namely, Honeypot based Dynamic Anomaly Detection using Cross Layer Security (HBDADCS) to detect the black hole attack in the network. Here, a dynamic timer algorithm was implemented for reducing the overhead of network. Also, the route lookup was utilized to dynamically invoke the detection process. In this paper, it was stated that the black hole attack could reduce the entire performance of the network by dropping the packets, so it must be detected by using an efficient technique.

Hemalatha and Bhuvaneswaran [22] introduced an energy aware multi path routing technique for improving the link stability of the network. The motive of this work was to reduce the overhead and ensure the minimum packet loss during communication. In this environment, the lifetime of the network was enhanced by considering the measures of battery management, transmission power, and system power management. During simulation, the speed of the suggested protocol was evaluated by estimating the delay time of the packets. The limitation that observed from this paper was, it required to improve the overall efficiency of the network by detecting the malicious activities of the nodes. Maheswari and Nedunchezian [6] utilized a Balanced Reliable Shortest Route (BRSR) – AOMDV protocol for balancing the load in the network in order to maintain the link stability. Here, the average queue length and signal strength were estimated for enabling the packet transmission in a reliable way. Also, the optimized path was selected by determining the average queue size of the neighbor. Moreover, the lifetime of the whole network was predicted based on the stability analysis of the nodes. However, this work required to increase the QoS of the network with improved security.

Pandey [23] analyzed the link stability of the network by increasing the robustness and maintaining the topology of the network. For this purpose, an On-Demand Multicast Routing Protocol (ODMRP) was developed for identifying the stability factor of a node. Also, two types of stability that includes neighbor stability and path stability were analyzed for ensuring a path consistency from source to destination. Here, the most stable route between the nodes identified by estimating the stability function. The major limitations of this work reduced throughput and increased delay. Xu and Li [24] implemented an energy aware routing with tradeoff strategy for identifying the breaking links in the route with increased stability. The major focuses of this work reduced the packet loss and routing overhead during packet transmission. Here, the node energy and traffic were balanced for increasing the packet delivery ratio even in the high mobility condition. But, this work failed to detect the malicious activities in the network during communication. Singh *et al*., [25] investigated some routing protocols for analyzing the most suitable one in order to provide a reliable communication. The protocols that investigated in this work were as follows: table driven routing, on-demand routing, and hybrid routing. Also, the authors examined the advantages and disadvantages of all these protocols. Roy and Roy [26] introduced a stable multipath routing strategy for increasing the throughput of the network. Here, the node was selected based on its energy and link expiration time. In this environment, the route was established between the nodes with respect to varying time stamp value. However, this work failed to enhance the performance of this data delivery model with multipath strategy. Liu and Yu [27] implemented an Authenticated Anonymous Secure Routing (AASR) protocol for detecting the adversaries in the network. The

motive of this work was to authenticate the route request packets based on the group signature. Then, the intermediate nodes were prevented with secure route verification mechanism. The drawback that observed from this work was, it required to improve the performance of the network detection. Gandhi and Jhaveri [28] introduced a Fuzzy Trust based Secured Routing (FTSR) mechanism for analyzing the misbehavior of the nodes in MANET. Also, the behavior of the nodes was analyzed by applying the fuzzy operator. Here, the trust value was mainly calculated by considering the capacity and energy level of the nodes. The secure route was discovered by securely evaluating the routes in the network.

Jain and Buksh [29] suggested some solutions to enable a secure routing in MANET by considering the measures of cost, resource usage, and QoS. Here, different routing protocols that used for routing discussed which includes proactive, reactive, and hybrid. In this work, it was stated that the enabling a secured environment in MANET against the harmful attacks was one of the difficult task due to the characteristics of MANET. Anand and Jayakumar [30] developed a Dynamic Province based Route Selection Algorithm (DPBRSA) for detecting the black hole attacks in MANET. In this paper, the Bee Colony (BC) optimization technique was implemented to perform the route discovery and route maintenance processes. Here, the energy level of the nodes was estimated before enabling the communication. Moreover, the malicious path in the route was determined for ensuring the increased PDR. However, this work required to prove its efficacy of the suggested system by evaluating different performance measures.

From the survey, it is studied that the traditional techniques have both benefits and drawbacks, but it mainly lacks with the following limitations:

- Increased overhead and latency
- Computational complexity
- Minimized attack detection rate
- Single stage detection process
- Not highly efficient

In order to solve these problems, this paper aims to develop a new attack detection mechanism with link failure analysis for enabling a reliable communication in MANET.

3. PROPOSED METHOD

In this sector, the detailed description about the proposed methodology is presented. The main motive of this paper is to provide security to MANET against black hole and gray hole attacks with improved link stability. For this purpose, a Secure Link Aware Fault Detection (SLAFD) mechanism is proposed in this work, which aims to detect the packet dropping attacks in an efficient manner. The flow of the proposed system is depicted in Fig. 2, which includes the following stages:

- Neighbor discovery
- Route discovery
- Attack detection

- Link analysis
- Secure packet transmission
- Link fault detection

At first, the network is formed with the set of mobile nodes, where the neighbor discovery is performed by sending the HELLO packets to the nearest nodes. Then, the RREQ is forwarded to the neighboring nodes which are in the range of < 200m, and the request is spread out to the other nodes that nearer to the neighboring nodes.

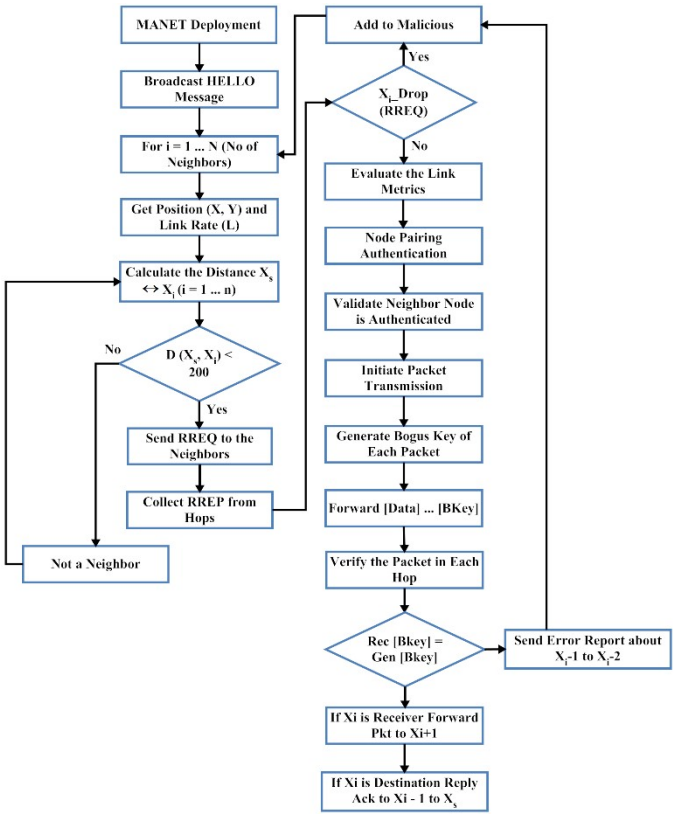

Fig. 2. Flow of the proposed work.

After that, the attacker nodes are detected and added in the suspected list, if the source does not receive any response or it receives the same RREQ. Furthermore, the route between the trustworthy nodes is formed by checking the link stability with the use of Genetic Algorithm. Then, the packets are transmitted between the authenticated nodes with the use of bogus key. The data to be transmitted are split based on the window size which can be formed as a packet. Each packet generates the bogus key for the purpose of security. Initially the key is compared with the window size and if the key is greater than the window size then it can be shortened with the help of hash function. Now the size of the key becomes the bogus key size. If the key is smaller than window size, it can be

padded with zeroes in order to make it as the size of window. Then the inner padded key and the outer padded key are computed by exploring the key with window size. Finally the hash keys are returned as the bogus key. By transmitting the data packet and bogus key separately, it is difficult to access both the data and control packets for the compromised node. Also the node authenticity is validated by the intermediate nodes pairing. This offers some benefits such as more security in data transmission, highly efficient, reliable due to the nature of scalability. After the data packet is transmitted, the compromised nodes are detected and blocked for further communication process. Here, the jitter is estimated between the intermediate nodes for detecting the compromised nodes and link failures. The GA is also used to analyze the faulty links in the network for enabling an error free communication with increased packet delivery ratio.

A. Neighbor Discovery and Route Discovery

Initially, the network is formed with the set of mobile nodes, in which the neighbors are discovered by sending the HELLO packets. The reason of sending this message is to reduce the network overhead and network traffic. Here, the usage of the particular node for a certain amount of time is analyzed Based on the network configuration and topology, the neighborhood nodes that surround the source node are identified. Then, the source node broadcasts the RREQ to its neighboring nodes that are in the range of < 200m. The simulation set up for transmission range value is 250m, which is the maximum range. The minimum value is kept as 200m. If the nearest node once receives the request, it sends an acknowledgement RREP to the source for enabling a data communication.

B. Attack Detection

After discovering the route between the nodes, the attacker nodes are identified and blocked into the suspected list. In this environment, two harmful attacks that includes black hole and gray hole are detected before data transmission. In which, the black hole attack receives the data from the source node and does not forward it to other node. It is a kind of network layer attack that modifies or blocks the original packet. This type of attack is highly dangerous to the network, because it forms very week routing infrastructure. Moreover, the selfish nodes that may be a single or combination nodes are participated in the communication for reducing the network performance. Similarly, the gray hole is also one of the hazardous attack in the ad hoc network, which aims to drop the forwarded packets by refusing it during packet transmission. The detection of gray hole attack is difficult because, it behaves maliciously for the time until dropping the packets, then it switch to the normal behavior. So, both the black hole and gray hole attacks disrupt the network based on its malicious behavior. Thus, this work aims to detect these attacks before packet transmission, if there is any attack in the path, it automatically added into the suspected list. Then, the route between that nodes is blocked and the communication is not enabled.

Algorithm 1: Functional Steps of Source Node

Step 1: Begin beaconing to initiate the process of neighbor discovery;
Step 2: if (the *Src* sends the data) then
Step 3: t_s = set clock time (node (*Src*))

```
Step 4:  Initiate the route discovery procedure
Step 5:  Select the intermediate nodes based on the Distance ( ) < 200;
Step 6:  Src selects a route (RTS) to Dst from its cache;
Step 7:  if (no route to Dst exist in its cache)
            Go to Step 4;
Step 8:  if (route contains the nodes belongs to the primary suspect list)
         {
            Relay nodes near to the accused nodes are switched ON to work in the pro-
            miscuous listening node;
         }
Step 9:  if (Current source node clock time t_s)
         mod check time = = 0)
         {
            Send routing table;
            Calculate link metrics of each node;
            Calculate overall link metrics of each path;
            Make entry in the routing table;
            Transmit the data packet with bogus key;
            Go to Step 6;
         }
Step 10: if (receives suspect list || malicious list)
         {
            If (receives suspect list)
            {
               Update primary suspect list
            }
            If (receives malicious information)
            {
               Update malicious list and primary suspect list;
            }
            If (end of data)
            {
               Do-nothing;
            }
            Else
            {
               Go to Step 6;
            }
            If (received RERR)
            {
               Go to Step 6;
            }
         }
Step 11: End if;
```

C. Link Analysis

After detecting the attacks, the route between the trusted nodes is enabled by using the GA, which is mainly used to check the stability of the link during data transmission. Typically, the GA is a multipurpose algorithm that is mainly used for searching and optimization problems. It selects the best path based on optimization and analyze its stability for a secure communication. The operators that used in GA are selection, crossover, and mutation, which are used to identify the failure links in the route. The process of link path analysis is performed as follows:

Algorithm 2: Link Path Analysis

Step 1: Initialize the nodes;
Step 2: Compute the nearest neighbors based on RSSI and relative velocity;
Step 3: Estimate the queue size for each node;
Step 4: Compute the response time for each node;
Step 5: Compute the bandwidth required for data;
Step 6: Estimate the Link Quality Factor (LQF) based on the following formula;

$$LQF(S, D) = \sum_{i=0}^{n}(QS_i + RT_i + BW_i - IR_i)$$

$$Qs_i = \frac{Total\ Queue\ Size - Ocuupied\ Queue\ Size}{Frame\ length}$$

$$RT_i = (T_{DERX} - T_{DDTX}) + (T_{ACKETX} - T_{ACKDRX})$$

//Where, T_{DERX} − Time of Data Packet Enqueued in Rx_Port,
T_{DERX} − Time of Data Packet Dequeued in Tx_Port,
T_{ACKET} − Time of acknowledgment Packet Enqueued in Tx_Port,
T_{ACKDRX} − Time of acknowledgment Packet Dequeued in Rx_Port,
IR_i – Interference ratio and BW_i – Bandwidth;

Step 7: Arrange the nodes in the list based on LQF and RSSI neighbor;
Step 8: Construct list with the links;
Step 9: Perform Heuristic-based fitness search to compute the global values corresponds to the nodes having best LQF and RSSI;
Step 10: Extract the quality measures for each instant and then update the list;
Step 11: Repeat from step 8;

Here, the fitness function is evaluated for each population, in which the local best and global best values are identified. Then, the fitness function is estimated for the search results, and the global best corresponds to the fitness value is extracted. The searching operation is finished and the best QF is estimated once it reaches the maximum iteration. Based on this process, the link quality is analyzed and the route is established between the communicating nodes.

D. Secure Packet Transmission and Link Fault Detection

After analyzing the links between the nodes, the bogus key generation, and node authentication processes are performed in order to ensure a successful transmission. In this environment, the generated bogus key (*i.e.* control packet) and data packet are separately transmitted to the destination. So, the compromised node cannot easily access both the data and control packets. Moreover, the authenticity of the node is validated by pair-

ing the intermediate nodes. After transmitting the packet, the nodes that are compromised by the attackers are identified and blocked for further communication. Moreover, the faulty links in the routed path are also identified by using the GA. The detailed procedure of the secure data transmission and fault detection is illustrated in the following algorithm. Here, the total jitter T is the combination of random jitter (J_{rnd}) and deterministic jitter between node i and j ($J_{i,j}$). Also, the value of σ is based on the BER of the link, ρ indicates the number of packets that are successfully forwarded, and p is the number of forwarded packets.

Algorithm 3: Functional Step of Neighboring Node

Step 1: If (Data packet received) then
{
Prepare to forward the packets to the next neighbor;
If (Detects the link break)
Generate and send RERR to source;
End if;

Step 2: Calculate the Total Jitter between the sender and receiver nodes;
$J^T = \sum_{p=1}^{\rho} J_{i,j}(p) + 2 \times \sigma(p) \times J_{rnd}$;

Step 3: Calculate the average Jitter;
$J^A = J^T/\rho$
$J^c = J_{i,j}(c) + 2 \times \sigma(c) \times J_{rnd}$

Step 4: If ($-\Delta J^a + J^A < J^C < \Delta J^a + J^A$)
Promiscuous listening mode == OFF;
Else
Promiscuous listening mode == ON;
End if;

Step 5: If (Promiscuous == ON)
Monitor the forwarding behavior of its neighbors;
Generate bogus key for received packet;
If ($r(b_{key})! = g(b_{key})$)
Create packet that contains malicious information and sends it to the source;
Else
Set its own promiscuous listening mode == OFF;
Create packet to contain link status update and send it to the source;
End if;
If (neighbor != destination)
If (found its forwarder malicious)
Send (RERR) to source;
Else
Forward (Data) to neighbor;
End if;
Else
If (found its forwarder malicious)
Send (RERR) to source;
Else

```
                    Send (Ack) to neighbor;
                End if;
            End if;
Step 6: End if;
```

4. PERFORMANCE ANALYSIS

In this part, the simulation results of existing and proposed security based routing protocols are experimented by using the parameters of packet loss rate, link fault detection, average end-to-end delay, latency, packet delivery ratio, and throughput. In this evaluation, the Ns-2 simulation tools is utilized to analyze these measures. The experimental settings of this work are illustrated in Table 1.

Table 1. Simulation settings.

Parameters	Values
Simulation time	200 s
Topology size	1500 × 1300 m2
Number of nodes	> 100
Maximum power	0.8W
Pause time	3 to 5 s
Maximum speed	10 m/s
Traffic type	CBR/VBR
Packet size	1024 bytes
Wireless channel capacity	2 Mbps
Routing protocol	AODV and OLSR
Transmission range	250 m (limited 200m)
Mobility model	Random waypoint
Buffer size	256000
Wireless standard	802.11b

A. Packet Loss Rate

The packet loss is occurred when the packet sent by the source is not received by the correct destination due to the malicious activities of the attacks. Fig 3 shows the packet loss rate of existing SVC/AODV, SVC/QAODV, adaptive SVC/AQA and proposed SLFD techniques with respect to varying mobile nodes ranges from 20 to 120. In this evaluation, it is proved that the proposed SLFD provides the reduced packet loss rate, when compared to the other techniques. Because, it detects the harmful black hole and gray hole attacks at the beginning stage, and the routing path between the trusted nodes are validated by checking its link availability. So, the maximum packet loss is avoided in this network with the use of SLFD.

B. Link Fault Detection

The fault detection rate is evaluated by analyzing the faults or failures that occurred in the link during communication. Fig. 4 shows the link fault detection rate of both ex-

isting and proposed techniques with respect to varying mobile nodes. From this figure, it is analyzed that the link fault is efficiently minimized by analyzing its stability with the use of GA. So, the performance of fault detection is improved, when compared to the other techniques.

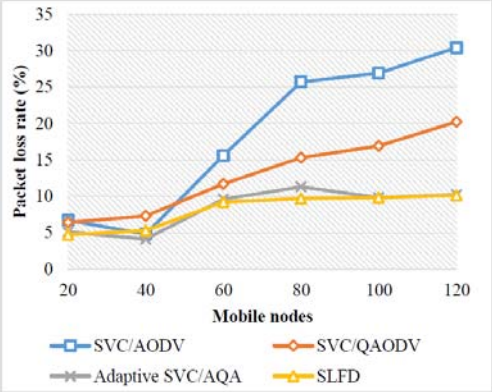

Fig. 3. Packet loss rate.

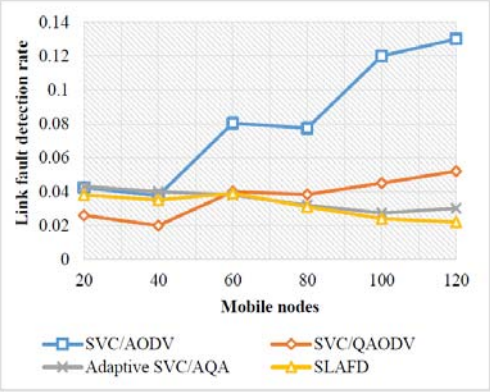

Fig. 4. Link fault detection.

C. Average End-to-End Delay

The end-to-end delay is defined as the required amount of time that a packet takes to travel from the source node to destination node. It is estimated as follows:

$$\textit{Transmission delay} = TR - TS. \tag{1}$$

Where, TR indicates the time when the message is received by the destination, and TS indicates the time when the message is sent by the source. Fig. 5 shows the end-to-end delay of both existing and proposed protocols with respect to varying mobile nodes that ranges from 20 to 120. In this analysis, it is proved that the proposed SLFD provides a minimum transmission delay, when compared to the other techniques. Because, it estimates the jitter between the intermediate nodes during packet transmission.

D. Latency

Latency is defined as the amount of time that a system holds a packet in the network, where the system may be a router or an entire communication system. Fig. 6 shows the latency of existing and proposed techniques with respect to varying mobile nodes ranges from 20 to 120. Here, the latency of the network is efficiently reduced, when compared to the other techniques. Because the jitter is estimated between the intermediate nodes during packet transmission where jitter is a delay that can vary over time, the compromised nodes are identified during this process which reduces the latency of the network.

E. Packet Delivery Ratio

The PDR is estimated based on the division of the number of packets transmitted by a source node and the number of packets received by a destination node. It is mainly to evaluate the adeptness and exactness of the routing protocols by estimating the loss rate.

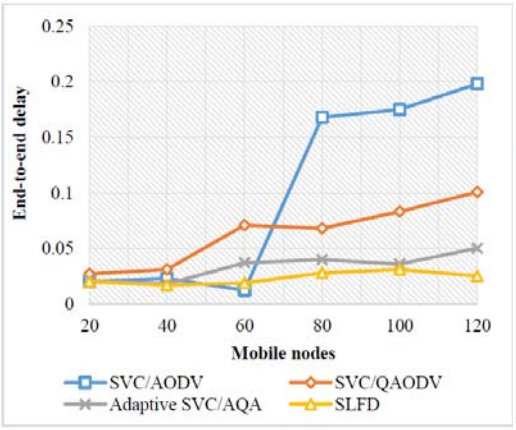

Fig. 5. End-to-end delay.

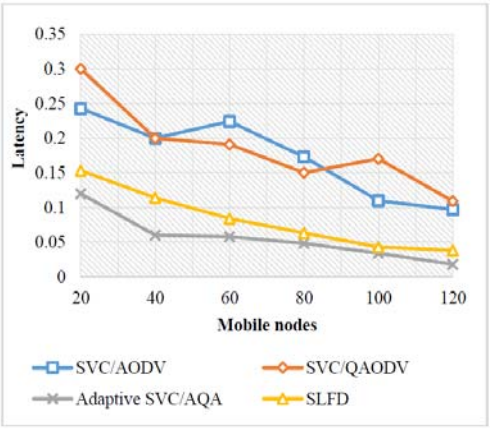

Fig. 6. Latency.

Fig. 7 shows the PDR of the existing and proposed protocols with respect to varying mobile nodes that ranges from 20 to 120. The PDR is calculated as follows,

$$PDR = \frac{Number\ of\ packets\ received}{Number\ of\ packets\ transmited} * 100.$$

The existing techniques that considered in this simulation are SVC/AODV, SVC/QAODV, and adaptive SVC/AQA. When compared to these techniques, the proposed SLFD provides the increased PDR by avoiding the link failures and detects the attacks before enabling the transmission.

F. Throughput

The throughput is defined as the successful rate of data delivery over the secure routing medium. Fig. 8 shows the analysis of throughput for both existing and proposed methods with respect to varying mobile nodes that ranges from 20 to 120. In this evaluation, it is proved that the proposed SLFD technique has an increased throughput, when compared to the other techniques. Because, it performs the neighbor discovery based on

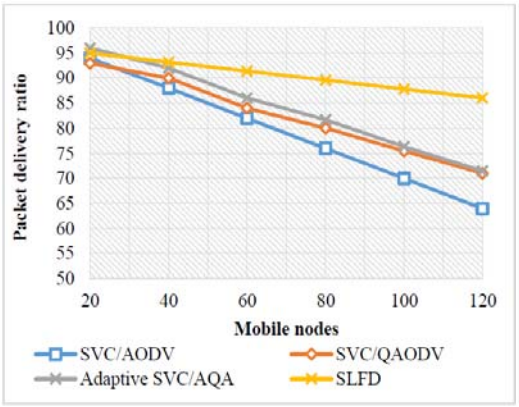

Fig. 7. Packet delivery ratio.

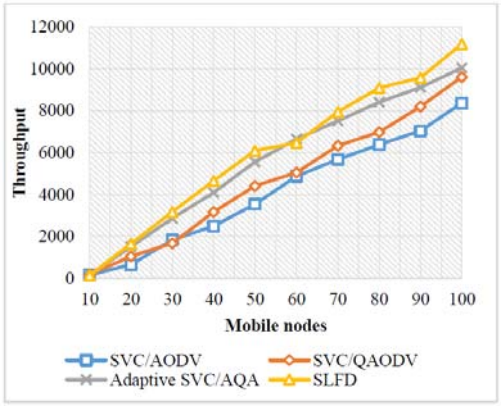

Fig. 8. Throughput.

the distance < 200m and, it identifies and avoids the link failures during communication by using GA.

5. CONCLUSION AND FUTURE WORK

This paper aims to develop a secure link stability analysis for providing a fault free communication in MANET. For this purpose, a SLFD technique is proposed in this work, which considers the objectives of both link fault detection and attack identification. Here, the neighbor discovery and route discovery processes are performed by analyzing the distance between the nodes. Then, the black hole and gray hole attacks in the network are identified and blocked before enabling a data transmission. It improves the efficiency of network with increased packet delivery rate and QoS. Then, the link path is validated by the use of GA, in which the stability of the routing path is analyzed. Also, the bogus key generation and node authentication processes are performed for allowing an authenticated nodes during packet transmission. Moreover, the link faults are identified by calculating the jitter, which is estimated between the intermediate nodes. Finally, the faults in the links are identified by using GA, which ensures an error free path for data transmission. During simulation, different experimental measures are used to analyze the performance of the proposed SLFD technique. Also, its superiority is proved by comparing it with the existing techniques. From the results, it is validated that the proposed SLFD provides the better results, when compared to the other techniques.

In future, this work can be enhanced by implementing the swarm intelligence method for detecting the selfish nodes in the network in an accurate manner.

REFERENCES

1. A. S. Nargunam and M. Sebastian, "Fully distributed security architecture for MANET," *International Journal on Information Technology*, Vol. 2, 2014, pp. 168-176.
2. R. Singh and D. Kumar, "MANET: Security issues and behavior analysis of routing protocol using NS-2," *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 5, 2015, pp. 241-251.
3. M. Chitkara and M. W. Ahmad, "Review on manet: characteristics, challenges, imperatives and routing protocols," *International Journal of Computer Science and Mobile Computing*, Vol. 3, 2014, pp. 432-437.
4. A. K. S. Ali and U. Kulkarni, "Characteristics, applications and challenges in mobile ad-hoc networks (MANET): Overview," *Wireless Networks*, Vol. 3, 2015, pp. 6-12.
5. M. L. Raja and C. D. S. S. Baboo, "An overview of MANET: Applications, attacks and challenges," *International Journal of Computer Science and Mobile Computing*, Vol. 3, 2014, pp. 408-417.
6. D. Maheshwari and R. Nedunchezhian, "An optimized approach on link stability with load balancing in MANET using balanced reliable shortest route AOMDV (BRSR_AOMDV)," *Indian Journal of Science and Technology*, Vol. 9, 2016.
7. H. Xia, *et al.*, "Applying link stability estimation mechanism to multicast routing in MANETs," *Journal of Systems Architecture*, Vol. 60, 2014, pp. 467-480.
8. D. Ahirwar and S. S. Rai, "Improvement of AODV routing protocol algorithm with

link stability and energy efficient routing for MANET," *International Journal of Science, Engineering and Computer Technology*, Vol. 4, 2014, p. 36.
9. K. J. Sarma, *et al.*, "A survey of black hole attack detection in MANET," in *Proceedings of International Conference on Issues and Challenges in Intelligent Computing Techniques*, 2014, pp. 202-205.
10. S. Brar and M. Angurala, "Review on grey-hole attack detection and prevention," *International Journal of Advance Research*, *Ideas and Innovations in Technology*, Vol. 2, 2016.
11. R. Ranjan, *et al.*, "Security issues of black hole attacks in MANET," in *Proceedings of International Conference on Computing*, *Communication and Automation*, 2015, pp. 452-457.
12. A. Dorri, *et al.*, "Security challenges in mobile ad hoc networks: A survey," *International Journal of Computer Science and Engineering Survey*, Vol. 6, 2015, pp. 15-29.
13. S. Brahmbhatt and A. Kulshrestha, "Study of route stability in MANET using quality of services," *International Journal of Computer Applications*, Vol. 119, 2015.
14. K. Gokila and V. Ila, "Heuristic based link quality preservation for reliable data delivery," *International Journal of Communication Systems*, 2017, p. e3304.
15. O. B. Rhaiem, *et al.*, "Qos improvement for video streaming over manet using network-coding," in *Proceedings of IEEE 82nd International Conference on Vehicular Technology Conference*, 2015, pp. 1-5.
16. S. Kumar, "Implementation of delay variance attack using video streaming in MANET," *International Journal for Light and Electron Optics*, Vol. 127, 2016, pp. 3303-3307.
17. W. E. Castellanos, *et al.*, "A QoS-aware routing protocol with adaptive feedback scheme for video streaming for mobile networks," *Computer Communications*, Vol. 77, 2016, pp. 10-25.
18. M. Malathi and S. Jayashri, "Robust against route failure using power proficient reliable routing in MANET," *Alexandria Engineering Journal*, Vol. 57, 2018, pp. 11-21.
19. T. Saeed, *et al.*, "Predictive activation for localization using minimal data-fusion in MANETs," in *Proceedings of the 5th International Conference on Information and Communication Technologies*, 2013, pp. 1-6.
20. M. K. Rafsanjani and H. Fatemidokht, "FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs," *AEU-International Journal of Electronics and Communications*, Vol. 69, 2015, pp. 1613-1621.
21. G. Usha, *et al.*, "Dynamic anomaly detection using cross layer security in MANET," *Computers and Electrical Engineering*, Vol. 59, 2017, pp. 231-241.
22. R. Hemalatha and R. Bhuvaneswaran, "Link-stability and energy aware multipath routing in MANET," *Research Journal of Applied Sciences*, *Engineering and Technology*, Vol. 8, 2014, pp. 2179-2186.
23. M. A. Pandey, "Link stability in mobile ad hoc network," *International Journal of Emerging Trends in Science and Technology*, Vol. 2, 2015, pp. 2330-2337.
24. B. Xu and Y. Li, "A novel link stability and energy aware routing with tradeoff strategy in mobile ad hoc networks," *Journal of Communications*, Vol. 9, 2014, pp. 706-713.

25. G. Singh, *et al.*, "Role of link expiration time to make reliable link between the nodes in MANETs: A review," *International Journal of Applied Engineering Research*, Vol. 11, 2016, pp. 5321-5325.
26. T. Roy and S. Roy, "A typical stable multipath routing strategy in MANET," in *Proceedings of International Conference on Emerging Trends in Informatics and Communication*, 2017, pp. 7-10.
27. W. Liu and M. Yu, "AASR: Authenticated anonymous secure routing for MANETs in adversarial environments," *IEEE Transactions on Vehicular Technology*, Vol. 63, 2014, pp. 4585-4593.
28. J. R. Gandhi and R. H. Jhaveri, "Packet forwarding misbehaviour isolation using fuzzy trust-based secure routing in MANET," *International Journal of Computer Applications*, Vol. 122, 2015.
29. A. Jain and B. Buksh, "Solutions for secure routing in mobile ad hoc network (MANET): A survey," *Imperial Journal of Interdisciplinary Research*, Vol. 2, 2016, pp. 5-8.
30. M. V. Anand and C. Jayakumar, "Province and energy based itinerary selection for secure routing in MANET using bee colony optimization," *International Journal of Advances in Engineering & Technology*, Vol. 836, 2016, p. 840.

K. Gokila in the Department of Electronics and Communications Engineering, PSG College of Technology, Coimbatore, Tamil Nadu, India. Research interest is a secure link aware fault detection algorithm for enabling a reliable communication in MANET.
E-mail: gokilaphd55@gmail.com.

Ila. Vennila in the Department of Electrical and Electronics Engineering, PSG College of Technology, Coimbatore, Tamil Nadu, India.