International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 18 (2017) pp. 7459-7465

Regression-based Link Failure Prediction with Fuzzy-based Hybrid Blackhole/Grayhole Attack Detection Technique

P. Rathiga
Research Scholar, Department of Computer Science,
Erode Arts & Science College, Erode, Tamilnadu, India.

Orcid: 0000-0002-2687-6241

Dr. S. Sathappan
Associate Professor, Department of Computer Science,
Erode Arts & Science College, Erode, Tamilnadu, India.

Orcid: 0000-0003-2522-3318

Abstract

Most of the conventional routing protocols in Mobile Ad-hoc Network (MANET) utilize the path until a link breaks or failures. During the path reconstruction, packets may be lost which can cause significant packet delivery ratio and throughput degradation. The previous researches such as FMQTMHDCR approaches were developed for only detecting the blackhole and grayhole attacks which allows the prediction of malicious nodes in the network. However, the prediction of link failures was not considered which may degrade the network performance. Hence in this article, a novel Link Failure Prediction (LFP) algorithm is integrated to the Dynamic Source Routing (DSR) protocol. In this approach, a linear regression model is applied on the Received Signal Strength (RSS) of each node for predicting the link failure time. Once the link failure time is predicted, a warning is transmitted to the source node if the link is soon-to-be-broken or failure. Then, the source node can reconstruct the new route before the links failure time. The simulation results show that the proposed mechanism known as FMQTMHDCR-LFP can significantly increases the packet delivery ratio, throughput, normalized routing overhead and reduces the packet drop rate. Also, this approach prevents the blackhole and grayhole attacks in the network.

Keywords: Mobile ad-hoc network, Routing protocols, Link failure, Blackhole/grayhole attacks, Dynamic source routing, Linear regression, Received signal strength.

INTRODUCTION

Generally, a Mobile Ad-hoc Network (MANET) is a dynamically self-organizing network without any central administrator or infrastructure support. If two nodes are not within the transmission range of each other then, the other nodes are required for serving as intermediate routers for the communication between such two nodes. Moreover, the mobile devices move autonomously and communicate through dynamically changing network [1]. Therefore, the frequent changes of network topology are a complex challenge for several significant issues like routing protocol, robustness and performance degradation resiliency. Proactive routing protocols require nodes for exchanging the routing information at regular intervals and determining the paths continuously between any nodes in the network regardless of using the paths or not. This refers a lot of network resources like energy and bandwidth can be dissipated which is not desirable in MANET where the resources are constrained. On the other hand, reactive protocols such as on-demand routing protocols does not require exchange of any routing information regularly. As an alternative, they discover the path only when it is required for the communication between two nodes.

The links between the nodes are temporary and not permanent due to the dynamic changes of network topology changes. For instance, a node cannot transmit packets to the intended next hop node and as a result packets may be lost. So, the route performance may be affected in different ways due to the loss of packets. Among these packet losses, loss or route reply provides more issues since source node requires re-initiating route discovery process. Additionally, node mobility may cause link failure and disruption in the active path which is utilized for transmitting the data from source to destination. Once the path is failure, the routing protocol has to repair the failure path or discover an alternative path. For an example, Dynamic Source Routing (DSR) protocol requires that the header of each routed packet should be carried a complete ordered list of nodes through which it moves. Upon link failure, the upstream node of the failure link transmits the Route Error (RERR) message to the source. Once RERR message is received, all paths containing the causing node will be eliminated from the source node cache. Then, the source will initiate a new path discovery or utilizes an alternative path from caches [2]. Different mechanisms have been developed to tackle the link failure issues in MANET; mostly by keeping more backup path to be utilizes when path failure happens. However, the chances of utilizing the backup paths are very low. Therefore, the link failure prediction is used which allows restoration of the active path before the current active path becomes unavailable. This will help to reduce the data packet loss and improve the network performance.

In previous researches, both blackhole and grayhole attacks were detected by computing data-to-control packet ratio based on the fuzzy based mobility, queue delay and traffic measurement which is known as FMQTMHDCR approach [3]. This approach improves packet delivery ratio and removes the failure of packet transmission by selecting an optimal path without any malicious nodes. However, the link failure was not predicted which may cause high packet drop rate. Hence the major objective of this research work is to propose a mechanism that tackles the issues related with the link failure and route maintenance in the previous researches. In the proposed approach, the link failure prediction algorithm is integrated to the DSR protocol. A linear regression model is applied on the received signal power strength for predicting the link failure time and transits a warning to the source node if the link is soon-to-be broken. Thus, the link failure is predicted in earlier and prevents the packet loss which improves the packet delivery ratio and routing performance.

The rest of the article is organized as follows: Section 2 provides the different link failure prediction approaches based on the estimation of link stability, mobility, etc. Section 3 describes the proposed link failure prediction approach using regression model. Section 4 illustrates the performance evaluation of the proposed approach compared with other approaches. Section 5 concludes the research work.

LITERATURE SURVEY

Ad-hoc On-demand Distance Vector (AODV) routing overhead [4] was analysed based on the link failure probability in MANET. In this approach, the collision probability which is caused by hidden-node issue and the impact on the link failure probability were analyzed. A mathematical analysis of the theoretical routing overhead of AODV protocol was presented according to the link failure probability. However, the maximum routing overhead was high and also only two scenarios were discussed such as chain and rectangle scenarios with all nodes stationary.

Link stability based multicast routing mechanism [5] was proposed in MANET. In this approach, a mesh based multicast routing protocol was proposed for finding the stable multicast route from source to destination. The multicast mesh was built by using route request and route reply packets with the help of multicast routing information cache and link stability dataset which is maintained at each node. The stable routes were identified based on the selection of stable forwarding nodes that have high stability and link connectivity. The link stability was estimated based on the parameters such as received power, distance between neighboring nodes and link quality. However, the scalability and flexibility were not improved.

Link stability estimation mechanism [6] was proposed for multicast routing in MANET. The major contribution of this approach was providing the stable connection service with the lowest communication cost. A novel link stability estimation framework was proposed based on the sampling of received signal strength information. In this approach, the proposed model was integrated with Multicast AODV which is used for discovering more available stable paths and adapting to network topology changes. However, the estimation of link expiration time was required for further improving the efficiency of finding more stable routes.

Fuzzy-Cost based Multi-constrained QoS Routing (FCMQR) [7] was proposed with mobility prediction in MANET. This FCMQR was used for selecting an optimal path by considering multiple independent QoS metrics such as bandwidth, end-to-end delay and the number of intermediate hops. This approach was based on the multi criterion objective fuzzy measure. All available resources of the path were converted into a single metric fuzzy cost. Mobility prediction was achieved for finding the lifetime of the path. An optimal path was selected based on the maximum lifetime and minimum fuzzy cost. However, the other QoS parameters such as delay jitter, buffer length and power consumption rate were not considered.

Multi-objective OLSR for proactive routing [8] was proposed in MANET with delay, energy and link lifetime prediction. In this approach, three objectives were considered such as minimizing an average end-to-end delay, maximizing network energy lifetime and maximizing packet delivery ratio. As a result, three routing metrics were developed such as mean queuing delay on each node, energy cost on each node and link stability on each link. In this approach, queuing delay and energy consumption were predicted by using double exponential smoothing and the residual link lifetime was predicted by using a heuristic of the distributions of the link lifetimes in MANET. However, packet delivery ratio was less and the complexity of the method was high.

Link availability prediction based reliable routing [9] was proposed for MANET. In this approach, a novel Link availability Based Routing Protocol (LBRP) was proposed for MANET. An analytical expression of link availability for MANET was derived by using probabilistic and statistical computing. This approach was proposed based on random walk mobility model which is a continuous time stochastic process that characterises the random movement of nodes in a two-dimensional space. However, the complexity of the approach was high.

Link stability estimation [10] was proposed based on the link connectivity changes in MANET. In this approach, a novel scheme was proposed for estimating the link stability according to the link connectivity changes which may be performed on the network layer. A variable sized sampling window was adopted and the method was proposed for estimating the link transition rates. Then, the routing method was proposed for adjusting its operating mode based on the estimated link stability. However, the fluctuation of the sampling window length was not reduced and the complexity of the method was high.

PROPOSED METHODOLOGY

In this section, the proposed link failure prediction approach (FMQTMHDCR-LFP) is explained in brief. This proposed mechanism aims at maintaining the active routes by utilizing an effective link failure prediction approach based on the linear regression model. The proposed link failure prediction algorithm predicts the link failure time between two mobile nodes in an active route. Initially, the source node power level is assumed to be constant. Received signal power samples are measured by the packets at the destination node which are transmitted from the source node. By using this information, the rate of change for a particular neighbor node's signal power level is calculated. The time when the signal strength level drops below the acceptable value is predicted based on the fixed signal power threshold.

In this approach, an optimistic radio transmission model is used. Consider node A has a communication range with radius R. If node B is located within this communication range, it is assumed to correctly receive the packets from node A. Therefore, the link availability of two mobile nodes can be easily computed by the distance between them.

Estimation of Received Signal Strength

Two-ray ground reflection approximation is used as a radio propagation model [11]. The movement of node B from the node A is shown in Figure 1.

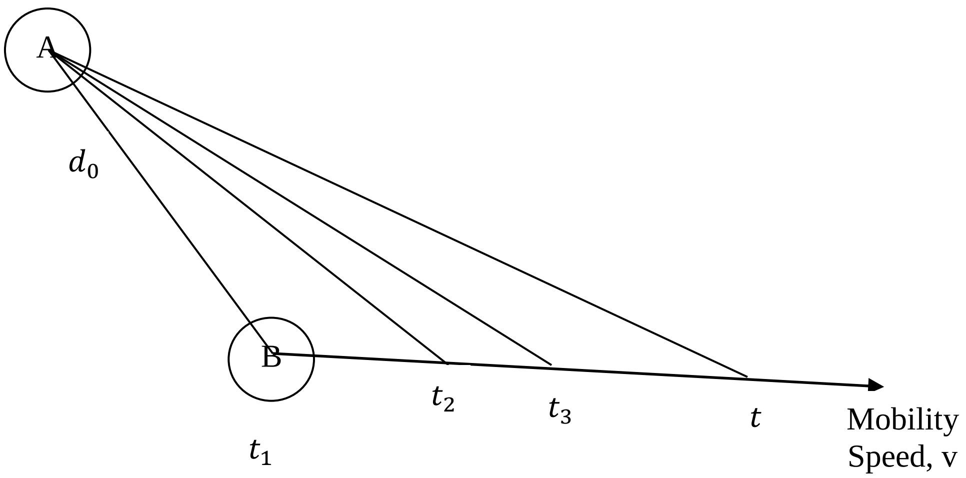

Figure 1: Relative Movement of Two Mobile Nodes

The following assumptions should be satisfied for the algorithm for predicting the link failure:

- The sender node power level is fixed.
- Two neighbor nodes keep their mobility speeds and directions during the prediction time.

When node A receives three consecutive radio signal powers from node B, then the link failure time between nodes A and B can be predicted as follows:

$$t = \frac{\sqrt{b^2-4ac}-b}{2a} \quad (1)$$

Where $a = t_2\sqrt{P_2 P_s}\beta$

$$b = \sqrt{P_s}\left(\left(\sqrt{P_1}-\sqrt{P_2}\right) - t_2^2\sqrt{P_2}\beta\right)$$

$$c = t_2\sqrt{P_2 P_s} - t_2\sqrt{P_1 P_2}$$

$$\beta = \frac{\left(\sqrt{P_1P_2}t_2+\sqrt{P_2P_3}t_3-\sqrt{P_1P_3}t_3-\sqrt{P_2P_3}t_2\right)}{\sqrt{P_2P_3}\left(t_2t_3^2-t_3t_2^2\right)}$$

In the above equations, P_s refers the received signal power threshold and it is constant for the wireless network interface. The three consecutive signal powers received by node A from node B at times t_1, t_2 and t_3 are referred as P_1, P_2 and P_3 respectively. This prediction algorithm is performed by the nodes only when the distance between two nodes is larger than the crossover point for reducing the consumption power.

Each mobile node keeps the received signal power strength and reception time of three packets transmitted from the same neighboring node. When node B receives the packets from node A, it updates this information according to,

$$P_3 \le P_2 \le P_1 \ and\ t_3 > t_2 > t_1 \quad (2)$$

When two mobile nodes are moving nearer, the most recent signal power strength will be greater than the previous value. In this case, the most recent signal power value is set to P_1 whereas P_2 and P_3 is set to zero, no prediction is required. The prediction algorithm assumes that two nodes maintain their mobility speeds and directions during t_1 and prediction time

T. In addition, this algorithm assumes that there is no noise during packet transmission. Moreover, this prediction approach is improved by applying regression method on the received signal power strength [12]. The regression model can be involved by the following variables:

- The unknown parameter ρ, which may be represented as scalar or vector.
- The independent variable P
- The dependent variable t

Assume a regression model has the number of unknown parameters and independent variables then, the dependent variable or linear prediction function is given as follows:

$$P_i = \rho . t_i \quad (3)$$

$$\text{Where } \rho = \frac{Standard\ Deviation\ (\sigma)}{Mean\ (\mu)} \quad (4)$$

$$\mu = \frac{\sum t_i}{n}, \ \ \sigma = \frac{\sum (t_i - \mu)^2}{n-1} \quad (5)$$

In above equations, P_i denotes the received signal power strength for i^{th} node at time t_i, ρ refers the regression coefficient and n denotes the number of nodes. Based on the regression coefficient, the received signal power strength is estimated and repeated until it is lower than the received signal power threshold. Thus, the predicted received signal power strength is utilized for estimating the link failure time and preventing the route from link failure or breakage.

Algorithm:

1. Initialize n number of nodes
2. Assign t_i for initiating packet transmission
3. For each packet transmission do
4. Estimate the received signal power strength of each node
5. Use regression coefficient to calculate the minimum received signal power strength at time t_i for particular node
6. $If\,(P_i < P_s)$ then
7. Update received signal power strength values for each node
8. Compute link failure time using updated signal powers between two nodes
9. Predict the link failure time
10. Choose an alternate path for packet transmission

EXPERIMENTAL RESULTS

In this section, the performance of the proposed link failure detection approach is evaluated based on the network parameters like throughput, packet drop rate, packet delivery ratio and normalized routing overhead. The simulation parameters are given in Table 1.

Table 1: Simulation Parameters

Simulator	NS-2.35
DoS attack	Black/Gray-hole attack
Channel Type	Channel/Wireless Channel
Antenna Type	Antenna/Omni Antenna
Radio Propagation model	Propagation/Two Ray Ground
Radio Propagation range	250 meters
Link Layer type	LL
Interface queue type	Queue/ Drop Tail / PriQueue
MAC type	MAC/802.11
Protocol studied	DSR
Simulation area	1000*1000
Trace format	New wireless format
Node movement model	Random waypoint
Traffic type	CBR (UDP)
CBR rate	50 Kbps
Data Payload	512 bytes/packet
Number of nodes	50
Malicious nodes	10
Speed	50m/sec
Transmission rate	10 packets/sec
Simulation time	600 sec

The performance metrics are evaluated under two types of simulation scenarios such as follows:

1. Scenario 1: Fixed Mobility with varying number of malicious nodes
2. Scenario 2: Fixed number of malicious nodes with varying mobility of the nodes

Performance Metrics

- **Throughput:** Throughput is defined as the amount of data packets correctly received by the destination node per unit time. It gives the information about whether the data packets are correctly received by the destination nodes or not. It is measured in terms of Kilobits per second (Kbps).

$$Throughput = \frac{Number\ of\ transmitted\ packets}{Time\ taken}$$

- **Packet Drop Rate:** Packet drop rate is defined as the fraction of number of dropped data packets at the destination node to the total number of data packets generated at the source node.

$$Packet\ Drop\ Rate = \frac{Number\ of\ dropped\ packets\ at\ destination}{Total\ number\ of\ packets\ generated\ at\ source}$$

- **Packet Delivery Ratio:** Packet delivery ratio is defined as the fraction of total number of data packets successfully received at the destination node to the total number of transmitted data packets from the source node.

$$Packet\ Delivery\ Ratio = \frac{Total\ number\ of\ packets\ received\ by\ destination}{Total\ number\ of\ packets\ transmitted\ by\ source}$$

- **Normalized Routing Overhead:** Normalized routing overhead is defined as the fraction of total number of routing packets such as RREQ and RREP transmitted per data packet.

$$Routing\ Overhead = \frac{Total\ number\ of\ routing\ packets\ transmitted}{Total\ number\ of\ data\ packets\ received}$$

Analysis of Fixed Mobility with Varying Number of Malicious Nodes

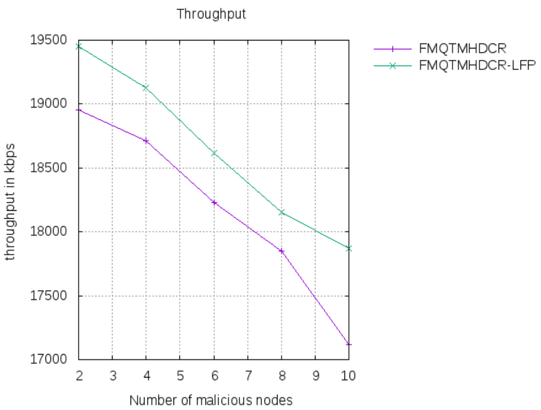

Figure 2: Comparison of Throughput (Kbps)

Figure 2 illustrates that the throughput comparison of FMQTMHDCR-LFP and FMQTMHDCR approaches for mobility speed of the node is 50m/s. In the graph, the number of malicious nodes are taken in x-axis and the throughput values (Kbps) are taken in y-axis. It shows that the proposed FMQTMHDCR-LFP approach has better throughput compared with FMQTMHDCR.

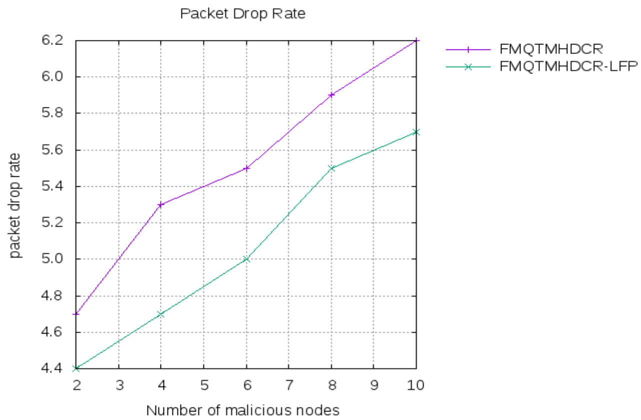

Figure 3: Comparison of Packet Drop Rate

Figure 3 illustrates that the packet drop rate comparison of FMQTMHDCR-LFP and FMQTMHDCR approaches for mobility speed of the node is 50m/s. In the graph, the number of malicious nodes are taken in x-axis and the packet drop rate values are taken in y-axis. It shows that the proposed FMQTMHDCR-LFP approach has reduced packet drop rate compared with FMQTMHDCR.

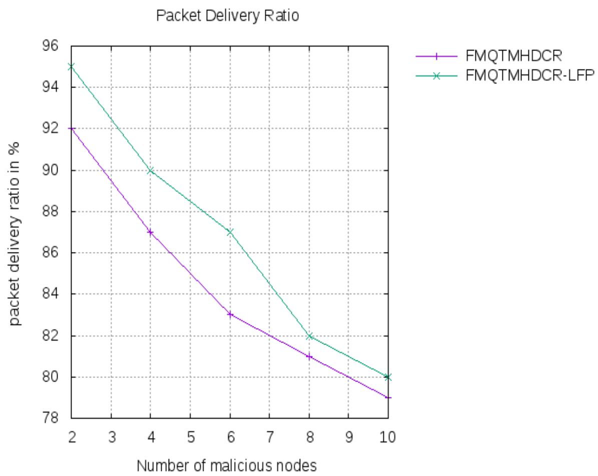

Figure 4: Comparison of Packet Delivery Ratio (%)

Figure 4 illustrates that the comparison of the packet delivery ratio for mobility speed of the node is 50m/s. In the graph, the number of malicious nodes is taken in x-axis and the packet delivery ratio is taken in y-axis. It proves that the proposed FMQTMHDCR-LFP approach has better packet delivery ratio compared with FMQTMHDCR.

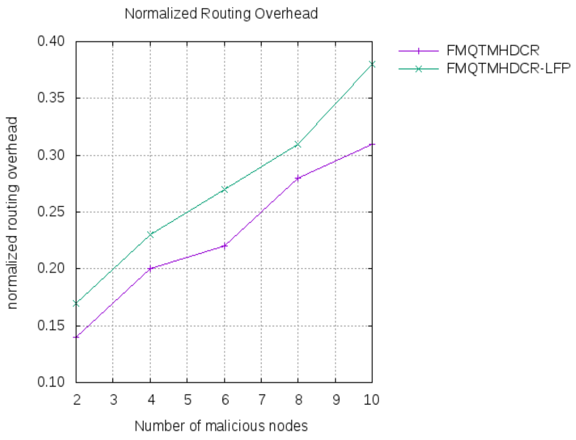

Figure 5: Normalized Routing Overhead

Figure 5 illustrates that the normalized routing overhead comparison of FMQTMHDCR-LFP and FMQTMHDCR approaches for mobility speed of the node is 50m/s. In the graph, the number of malicious nodes is taken in x-axis and the normalized routing overhead values are taken in y-axis. It shows that the proposed FMQTMHDCR-LFP approach has better normalized routing overhead compared with FMQTMHDCR.

Analysis of Fixed Number of Malicious Nodes with Varying Mobility of Nodes

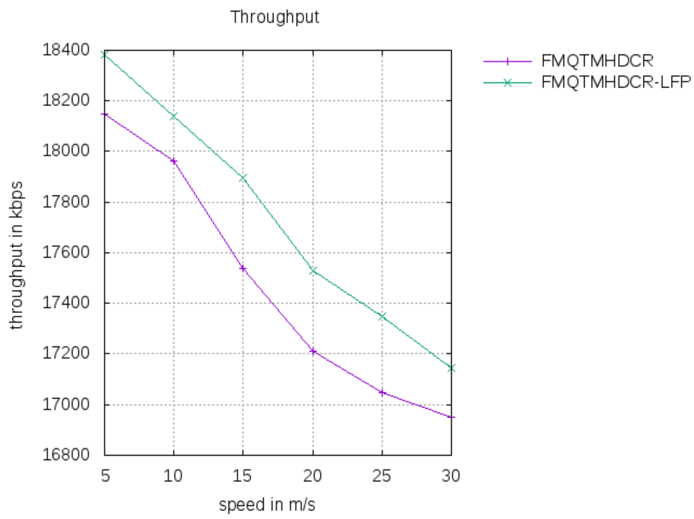

Figure 6: Comparison of Throughput (Kbps)

Figure 6 shows that the throughput comparison of FMQTMHDCR-LFP and FMQTMHDCR approaches where the number of malicious nodes are 10. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and the throughput values (Kbps) are taken in y-axis. It shows that the proposed FMQTMHDCR-LFP approach has better throughput compared with FMQTMHDCR.

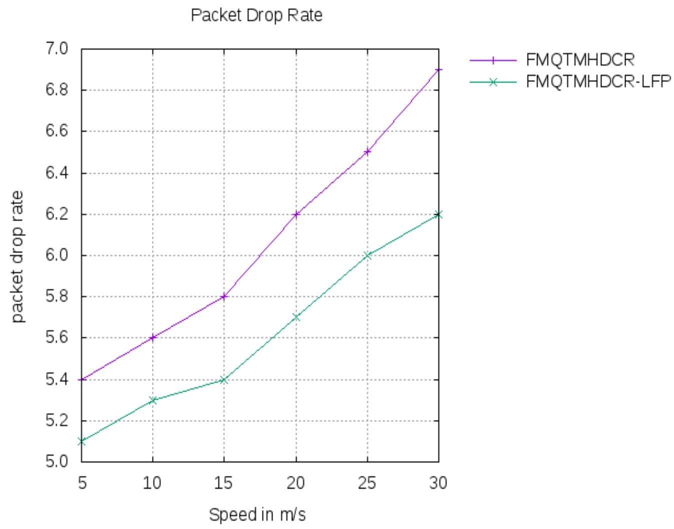

Figure 7: Comparison of Packet Drop Rate

Figure 7 shows that the packet drop rate comparison of FMQTMHDCR-LFP and FMQTMHDCR approaches where the numbers of malicious nodes are 10. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and the packet drop rate values are taken in y-axis. It shows that the proposed FMQTMHDCR-LFP approach has packet drop rate compared with FMQTMHDCR.

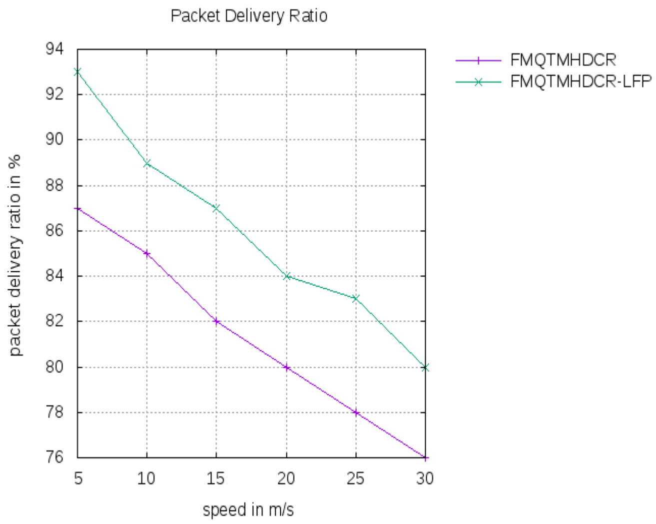

Figure 8: Comparison of Packet Delivery Ratio (%)

Figure 8 shows that the comparison of packet delivery ratio where the number of malicious nodes are 10. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and the packet delivery ratio is taken in y-axis. It proves that the proposed FMQTMHDCR-LFP approach has better packet delivery ratio compared with FMQTMHDCR.

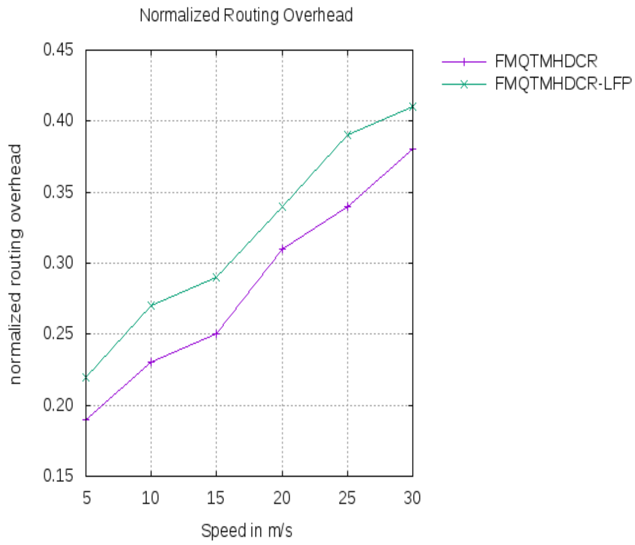

Figure 9: Comparison of Normalized Routing Overhead

Figure 9 shows that the normalized routing overhead comparison of FMQTMHDCR-LFP and FMQTMHDCR approaches where the number of malicious nodes are 10. In the graph, the mobility speed of nodes (m/s) is taken in x-axis and the normalized routing overhead values are taken in y-axis. It shows that the proposed FMQTMHDCR-LFP approach has better normalized routing overhead compared with FMQTMHDCR.

CONCLUSION

In this article, a novel link failure prediction algorithm FMQTMHDCR-LFP is proposed and integrated with the DSR routing protocol based FMQTMHDCR approach. This approach aims to overcome the issues related with the link failure and route maintenance in the conventional routing protocols in MANET. In this approach, a linear regression model is applied on the received signal power strength for predicting the link failure time and transits a warning to the source node if the link is soon-to-be broken. Thus, the utilization of signal power strengths of received packets predicts the active routes failure time in earlier and prevents the packet loss which improves the packet delivery ratio and routing performance. The simulation results prove that the proposed FMQTMHDCR-LFP approach reduces the packet loss rate, end-to-end delay and increases packet delivery ratio.

REFERENCES

[1] Shrivastava, R., and Malik, V., "An algorithm for improvement of link failure in mobile ad-hoc network," International Journal for Science and Emerging Technologies with Latest Trends, 10(1), pp. 15-18, 2013.

[2] Kadhum, M. M., "Innovative route maintenance based on link failure prediction for mobile ad hoc networks," In International Telecommunication Networks and Applications Conference (ITNAC), pp. 59-64, 2015.

[3] Rathiga, P., and Sathappan, S., "An effective secure mechanism using fuzzy hybrid DCR approach for MANET," Automatika: Journal of Control, Measurement, Electronics, Computing and Communications, 2017. (Submitted)

[4] Zhang, Q. J., Wu, M. Q., Yan, Z. H. E. N., and Shang, C. L., "AODV routing overhead analysis based on link failure probability in MANET," The Journal of China Universities of Posts and Telecommunications, 17(5), pp. 109-115, 2010.

[5] Biradar, R., Manvi, S., and Reddy, M., "Link stability based multicast routing scheme in MANET," Computer Networks, 54(7), pp. 1183-1196, 2010.

[6] Xia, H., Xia, S., Yu, J., Jia, Z., and Sha, E. H. M., "Applying link stability estimation mechanism to multicast routing in MANETs," Journal of Systems Architecture, 60(5), pp. 467-480, 2014.

[7] Santhi, G., and Nachiappan, A., "Fuzzy-cost based multiconstrained QoS routing with mobility prediction in MANETs," Egyptian informatics journal, 13(1), pp. 19-25, 2012.

[8] Guo, Z., Malakooti, S., Sheikh, S., Al-Najjar, C., and Malakooti, B., "Multi-objective OLSR for proactive routing in MANET with delay, energy, and link lifetime predictions," Applied Mathematical Modelling, 35(3), pp. 1413-1426, 2011.

[9] Han, Q., Bai, Y., Gong, L., and Wu, W., "Link availability prediction-based reliable routing for mobile ad hoc networks," IET communications, 5(16), pp. 2291-2300, 2011.

[10] Song, Q., Ning, Z., Wang, S., and Jamalipour, A., "Link stability estimation based on link connectivity changes in mobile ad-hoc networks," Journal of Network and Computer Applications, 35(6), pp. 2051-2058, 2012.

[11] Khazalah, F., Ababneh, I., and Malik, Z., "Forwarding group maintenance of ODMRP in MANETs," Procedia Computer Science, 19, pp. 289-296, 2013.

[12] Qin, L., and Kunz, T., "Pro-active route maintenance in DSR," ACM SIGMOBILE Mobile Computing and Communications Review, 6(3), pp. 79-89, 2002.