A Trusted Method For Early Data Link Failure Prediction

G. Jegan, D. Kamalakkannan, P. Samundiswary

Abstract*: Mobile ad-hoc network was widely used in the various fields for several applications. In the field of the wireless sensor network the link failure prediction is still a baffling one. The proposal here provides clear facts about the concepts of the link failure. In this paper the Proficient Trusted Node ID Based Resource Reservation Protocol (PT-NIDBRRP) was used. Here the shortest path was detected by using the weighted end-to-end delay based approach. This algorithm will find the short cut route from the particular starting place to the target and can improve the detection rate. By starting the route detection process the sequence numeral and the hop address is added to the protocol. After detecting the shortest path the link failure was detected. The link failure localization structure in the implemented trusted protocol has the higher ability in predicting and fixing the link failure issues. Then to find out the cause attack for the link failure the posterior probability estimation was used to sort out the type of the attack. At last the performance of the proposed method was evaluated through simulation analysis. The simulation result confirms that the proposed methodology is highly effective in detecting the link breakage and the short path algorithm implemented here will reduces the time period of detecting the shortest path. This method provides trusted secure network time duration, energy values and trust scores play an important role between the source and destination in the network.

Keywords: MANET, Proficient Trusted Node ID Based Resource Reservation protocol, weighted end-to-end delay based approach, Posterior probability estimation.

I. INTRODUCTION

In the networking technology the different kind of the attack is there which will try to reduce the growth of the networking technology. The networking attacks like stealing of the information, intruder intrusion, nodal venomous behavior, phishing, password theft, information alteration or destruction etc. The MANET was formed by the cluster of the nodes which can form a short-term network without the cluster heads. Hence any node can freely communicate with any node this behavioral condition in which easily the intruder can enters. Hence the MANET can easily subject to several kind of the attack when compared to the other networks. It can undergo attacks in several types of the methods. This condition can makes the MANAT an entrusted networking site. Hence the main problem blink on the MANET is the security issues and link breakage. The security side needs to be improved in the MANET.MANET suffered a lot due to the security problems because its an open resource and doesn't have defensive structure in their environment. Then in some time the nodes will gone unreachable because of the failure in the failure in the link. This kind of the failure will leads to the formation of the irregularity in the process. There are mainly two types of the failure in the wireless sensor network they are

- Failure occurs in more than one devices
- Failure in between the communication links

Mainly the failure in the link leads to the reduce in the throughput will leads to the deduction of the network growth. Unfortunately there will be none other effective diagnosis method for the detection of the link failure. In the several other existing methodologies the researchers mainly focuses on the malicious node and the attack detection. There will be some limited study related to the link failure analysis. This can induce the researchers to develop a highly reliable structure for link failure prediction. Here now we are going to develop a novel structure for enhancing the link failure prediction in MANET which will acts as a protective shield against the illegal conditions. The figure 1 represents the process of link breakage among the two nodes.

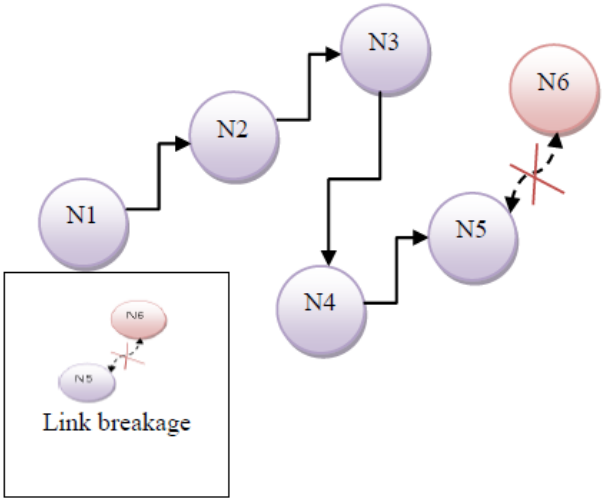

Fig.1. Link breakage between the nodes

II. LITERATURE SURVEY

Nandeep et al. (2017) [1] proposed a protocol which will find the link failure and the packet loses. The protocol can extract the least path and the route maintenance can done perfectly. Here if the protocol find out any breakage in the links means suddenly another route was preferred.

Revised Manuscript Received on January 15, 2020.

***** Correspondence Author

Dr. G. Jegan*, Department of ECE, MLR Institute of Technology, Hyderabad, India.
Email: jeganece84@gmail.com

Dr. D. Kamalakkannan, Department of ECE, MLR Institute of Technology, Hyderabad, India. Email: kamalakkannan_d@yahoo.com

Dr. P. Samundiswary, Department of Electronics Engineering Pondicherry, University, Puducherry, India

The main disadvantage of this method was its not a cost effective method. Ranjan et al. (2018) [2] proposed a novel selective mechanism. According to this method the particular nodes were selected for the process of carrying the information packets. Hence due to this selective mechanism the data loss reduces with decrease in the overhead and the power consumption. Pal et al. (2019) [3] applied a statistical model according to this model the node can determine fully about the neighbors after that only it can send the information packets to the neighbors. Then the BBO technique was applied to estimate the parameters of routing and this will estimate the routing path easily. Bandyopadhyay & Karforma, (2019) [4] proposed a method which was based on the fuzzy techniques for efficient short route selection and also for the process of the secure communication. Robinson et al. (2019) [5] proposed a novel neighbor Knowledge-based Rebroadcast algorithm for reducing the control overhead in the MANET. Pandey & Singh, R. (2019) [6] proposed a novel approach which is used for the purpose of modifying the routing protocols for enhancing its performance in the mobile ad-hoc network. Robinson et al. (2019) [7] proposed a novel method which was mainly depend which can predicts whether the link availability is present or not. Amiri-Doomari, S., Mirjalily, & Abouei, J. (2019) [8] proposed a Stability-based routing method which is used for the link scheduling and channel assignment in the MANET. Mahalakshmi, S& Vadivel, (2019) [9] proposed a novel method for detecting the shortest route for the process of the transmission of the information packets. Fatima et al. (2019) [10] proposed a prediction algorithm for determining the stability of the route. Prakasi, & Varalakshmi, P. (2019) [11] proposed a decision tree technique which was used for modifying the protocol for the purpose of finding the trusted route during communication. Calarany, & Manoharan, R. (2019)[12] proposed a efficient evaluation technique for determining the path stability in the MANET. Khanna et al. (2019) [13] proposed a trusted approach for determining the link expiration time and also the border time. Kumar, J., & Kathirvel, A. (2019) [14] make a analysis about the techniques which can improve the routing process in the MANET. Kumar & Babu, (2019, April) [15] proposed a simple cost effective attack detection method which will prove the computing intelligence in the MANET. Sharma, Alam, & Doja, (2019) [16] make a improvement on the DSR protocol using the ANFIS software. Kanellopoulos, (2019) [17] proposed about the recent developments in the process of improving the QoS in the MANET. Waheed, Wahid, & Shah, (2019, May) [18] proposed a aware method for predicting the link issues in FANET. Robinson et al (2019)[19] proposed a Link-Disjoint Multipath Routing for the purpose of monitoring and reducing the overhead in the MANET. Naresh, Raje, & Varsha, K. (2019, March) [20] proposed a novel link prediction algorithm for improving the process of the routing in the VANET. Sahu, Sharma, & Rizvi, 2019 [21] proposed a Zone Based Leader Election Energy Constrained AOMDV Routing Protocol for the purpose of power saving. Baskar et al [22], 2015 discussed about IP Based Adaptive Intrusion Tracing Mechanism for Detecting Low Rate DDoS Attacks

III. PROBLEM STATEMENT

Now a days many mobile ad hoc routing protocol will continue their communication process if there will be any break in the link. At a period of the reassembly of the route there will be a dropping of the information packets which will collapse the whole process of the communication. Hence dropping of the information packets will leads to the decrease in the throughput rate. This will reduce the growth of the network. So there is a imperative need for the search of an efficient method to overcome the data link breakage issues.

IV. PROPOSED METHODOLOGY

The proposed flow here focuses mainly on the detection of the data link breaks and determines the shortest path by using the implementation structure. The figure 2 represents the overall shortcut representation of the proposed flow of the work.

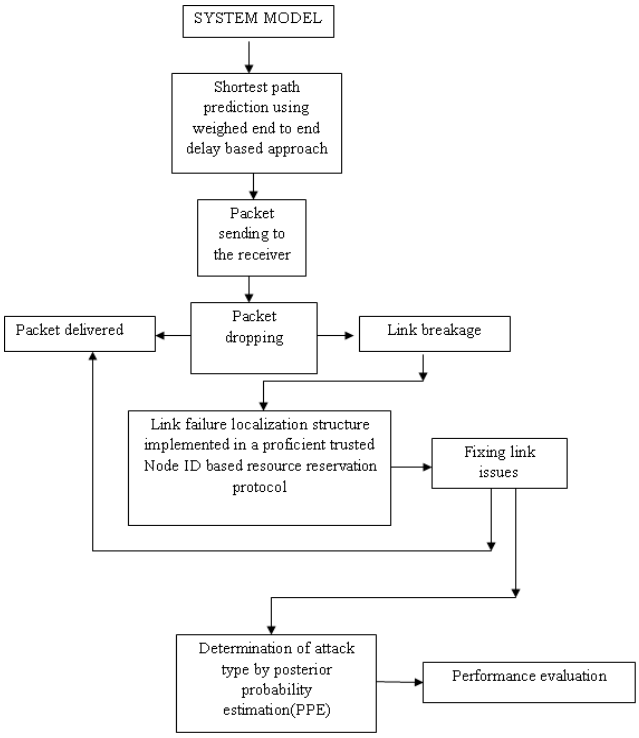

Fig.2. Schematic representation of the proposed methodology

A. System model

The mobile ad-hoc network is the wireless network which does not having the any kind of the infrastructure. Here mainly the nodes can communicate with each other thereby forming the multi-hop network. The data packets can send by the source node and then it can reach the destination node through number of the skips or jumps. The communication process will considered as a success one only there will be proper co-ordination among the nodes. First there will be several number of the nodes are there first they need to group hence the network gets divided into the interconnected sub structures after that the group will gets formed. There will be group head in each of the cluster. Each leader can plan a role of the base station within the group or the cluster.

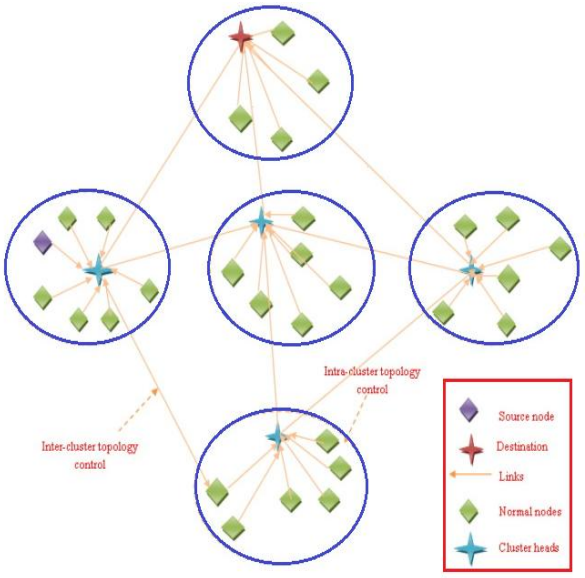

Fig.3. Planned architecture of the system model

The figure 3 represents the planned architecture of the implemented system model. The mobile gets form a cluster that all the nodes are having some group. Each group are separated not in a overlap form. The main function of the cluster was to maintan the key management system and mainly administers the group. This kind of grouping can mainly reduce the keys for the process of the communication. Each and every information packet can reach the cluster head before it reaches the destination source. The process of the clustering can be gone to improve the network security and to maintain the proper communication process.

B. Shortest path prediction using weighed end to end delay based approach

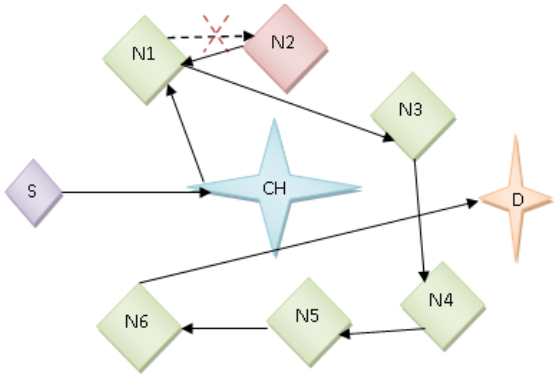

Fig.4. General existing methodology for sensor communication process

The figure 4 represents the general existing methodology of the process of the information transfer between the nodes. In the existing methods the information can send from the source node to the destination node .In case if there will be any malicious node present means the process gets stops and then again it will come to the source node and then it will restart the process. Initially it won't knows where should be the link breakage is present hence if again it start the process means there will be waste of the time and the energy. Hence there is a need to overcome the issues by implementing the weighed end to end delay based approach. The aim of this approach is to target the destination at a first attempt without losing the time and the energy. The weighed end to end delay is used for calculating the shortest path between the nodes. The delay was affected by the number of the hops in which a packet has to pass through. The hop length between the source and the destination keeps on changing with respect to the time. Here the protocol we used is the proficient trusted Node ID based resource reservation protocol. The routing protocol can be implemented for the particular network employment.

The end to end packet delay can be directly proportional to the length of the path. If the length of the path increases the end to end packet delay also gets increases. Here there will be a severe bonding between the path length and the packet delay. In the proposed weighed end to end delay approach in which the shortest path was calculated by finding out the weightage length of the path between each of the nodes from the source. The weighed path is the path with limited short distance and lack of the link break. After calculating the path the information packets can directly send to the destination node. It is somewhat a time saving process also saving the energy also.

C. Pseudo code for the shortest path selection using weighed end to end delay approach.

Procedure: Shortest path prediction
Inputs: Sequence number and Hops
Output: Shortest path from source to the destination
Step:1
Initialization of the hop parameters such as the communication range and number of the nodes.
Step:2
Obtain the minimal hop count information between each node
Step:3
Calculate average distance between the sensor nodes
Step:4
Computation of the estimated distance between the nodes
Step:5
Estimation of the nodal location
After calculating the distance between each node there is a need to search for a link breakage between the nodes. Because if there will be link breakage means again the information packet can come to the source and then regain the process. Hence for finding the link breakage the protocol used here was just modified and we are developed the proficient trusted Node ID based resource reservation protocol for easy prediction of the link breakage.

D. Proficient Trusted Node ID Based Route Reservation Protocol

The proficient trusted node ID base route reservation protocol will not provide any of the service for the network. The protocol in which the traffic characteristics between the sensor nodes was clearly explained. The PATH messages are sending from the source to the destination.

Here the messages are transmitted through several hops. Here each of the nodes was determined by its Id. The proficient trusted node ID based protocol is a route reservation protocol here in which the nodes are determined if it is necessary. Common messages are used to detect and monitor the links with the neighbors. If Common messages are used, each active node should periodically transfer a Common message to the entire neighbor node. If the nodes do not receive the common message from the neighbor the link gap was predicted. It generally uses the simplex flows through the network. The route message contains the information about the resources which is required for the connection. While the path message reaches the router the reservation process can begins. Then the inbound router sends the reservation message to the outbound user. After receiving the message the inbound user establish another unidirectional route. The path can simply open until the session was remains active. Here in which the quality of the service was guaranteed as well as the guaranteed bandwidth .It gave the guarantee on the packets but it does not provide guarantee in the delay variation. Mainly here the nodes ID can play an important role in this protocol depend upon the node id it can localize the node and find out the link break.

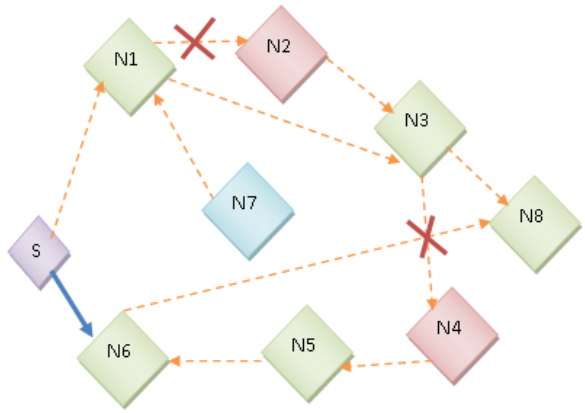

Fig.5. Proposed method of data transfer

The figure 5 represents the proposed method of detecting the short route lacking of the link breakage. Here assumed that the above scenario in which the source node is the starting point an N2 and N4is the malicious node and N7 is the cluster head and N6 is the destination node. Here there is link between each of the sensor nodes .By implementing the proficient trusted node ID based route reservation protocol with weighed end to end delay approach after the process of the analysis can be done after that it can be concluded that for N6 destination the weighted route was find out and the information can pass successfully on a first attempt. Generally it will save the time and energy.

E. Attack Estimation

The MANET was simply a open software in which it will subjected to different types of the attack. For determining the attack the posterior probability estimation method to be used .It is one of the probability distribution method used to determine the unknown prediction of the value and the process will depends upon the random variable selection. The main aim is it can search for a relevant background and randomly observe the relevant data. To achieve the goal there is a need to provide the regular interval .Simply it can observe the member probability and can reflect the value of the uncertainty.

Let us assume that the probability distribution of the variable can be calculated by using the Baye's theorem. It can be calculated by multiplying the probability distribution values and then the obtained value was divided by the normalizing constant.

$$P(\emptyset/x) = \left(p\frac{\left(\frac{x}{\emptyset}\right)}{p(x)}\right)P(\emptyset) \quad (1)$$

Where

$P(\emptyset)$ *is the probability distribution function ,*

$P\left(\frac{x}{\emptyset}\right)$ is the likelihood function

$P(\emptyset/x)$ is the evidence function

The posterior probability can be in the form of ,the posterior probability which is directly proportional to the likelihood which is a multiplication of the prior probability.

$F(x)=[f(x)\ (x/y=y(x)/\int_{-\infty}^{\infty} f(x)(u)L(x/y=y(x)(u)du]$ (2)

Where F(x) is the prior density function

f(x) L(x/y=y(x) which is a likelihood function

$f(x)(u)L(x/y=y(x)(u)$ is a normalizing constant

Basically the likelihood function was to map out the likelihood of the function. Then after finding the prior probability the attack was determined.

V. RESULTS AND DISCUSSION

Hereby we are implementing the weighed end to end delay method in the proficient trusted node ID based route reservation protocol and can undergone the process of the simulations. The result will be obtained in a higher accuracy because of the implementation of the proficient trusted protocol for the prediction of the link breakage. The main aim of this kind of the implementation is to find a short path without link breakage and to send a information packet to the destination in a single attempt. Hence in this section the overall performance of the proposed method was to be evaluated.

The following performance parameters are used to evaluate and compare the results and effectiveness of the proposed method.

A. **Packet delivery ratio**: Generally it the amount of the packets received by the receiver to the amount of the packets which can be transmitted by the sender.

$$P = (Pr / Ps) *100 \quad (3)$$

Here P is packet delivery ratio, Pr is the amount of packet received and Ps is the amount of packets sent.

B. Control overhead: It is the amount Number of manage packets developed for the amount of the data sent to the destination part .

C. Average end-to-end delay: It is the amount of the time consumed for the overall transmitting process and the overall delay of transmitting the messages that can be calculated.

$$AD = (Ps-Pr) / Pr \quad (4)$$

Here Ps is the packet sending time period and Pr is the packet received time period.

D. Throughput: The amount of data sent effectively in a single attempt during the process of the communication

E. Prediction of link break: It is used to identify the link breakage in the overall route.

F. Accuracy: Accuracy is the measure of the closeness of the obtained value to the standard value.

Accuracy (A) = (TP+TN)/(TP + TN + FP + FN) (5)

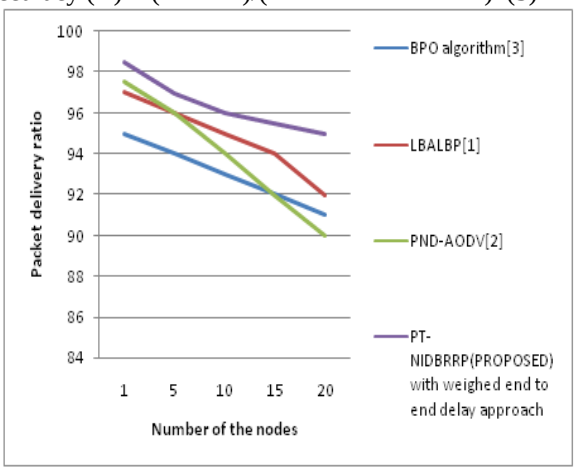

Fig.6. Number of the nodes Vs. packet delivery ratio

The figure 6 represents that the packet delivery ratio for the proposed protocol is higher when compared to that of the other existing protocol. This protocol can avoids the link breakage and can find the shortest path easily within a short period of time. During the process of the route recovery the protocol easily identifies the link break before the transfer of the data hence the data dropping was gradually reduced so that the packet delivery will automatically increase in amount.

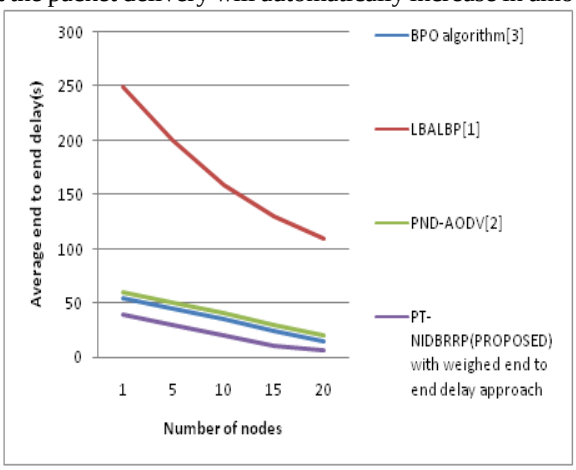

Fig.7. Number of nodes Vs. average end to end delay

The figure 7 represents that the average end to end delay of the proposed protocol is less when compared to the other existing protocol. Here the implementation of this protocol will avoids the over crowding process. Due to over crowding the large amount of packets gets dropped due to the confusion leads to the delay in the communication information transfer. And also if there is a break in the link the data can again resend to the source and then discover the new route and regain the process. But here in the proposed method before starting up the process the short route and the link breakage was discovered hence the information transfer in a first attempt. Hence here the time delay was avoided.

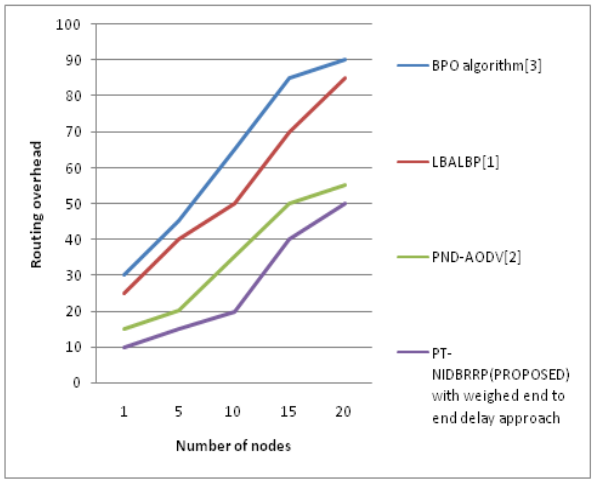

Fig.8. Number of nodes Vs. Routing overhead

The figure 8 represents that the routing overhead of the proposed protocol is less when compared to the other existing protocol. By finding the link break and the shortest path should find after that the message could be send. But there will be none other than more packets.

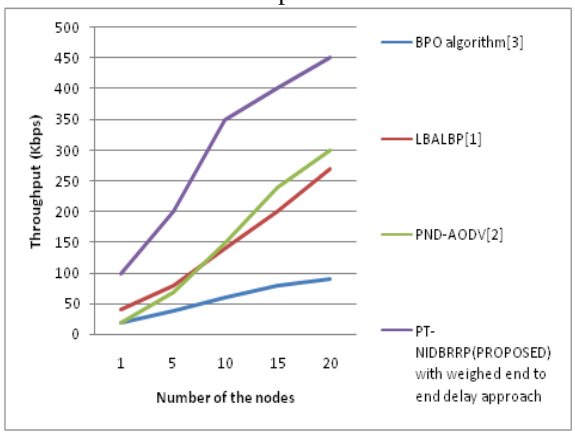

Fig.9. Number of the nodes versus throughput

The figure 9 represents that the proposed protocol gains more throughput ratio when compared to the all the other existing protocols. It can easily find out the link and the shortest path before the data can pass through the route. Hence it achieved a high throughput ratio.

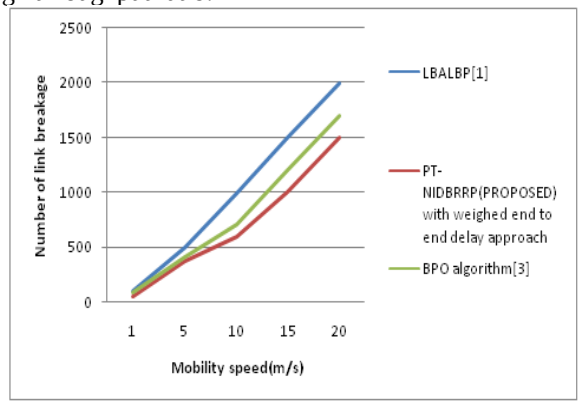

Fig.10. Mobility speed Vs. Link breakage

The figure 10 represents that the number of the link breakages in the proposed protocol is less when compared to that of the all the other existing protocols. The link breakage can be predicted before the process of the data communication. As the movement of the node increases then the link break occurs. Here that was overcome.

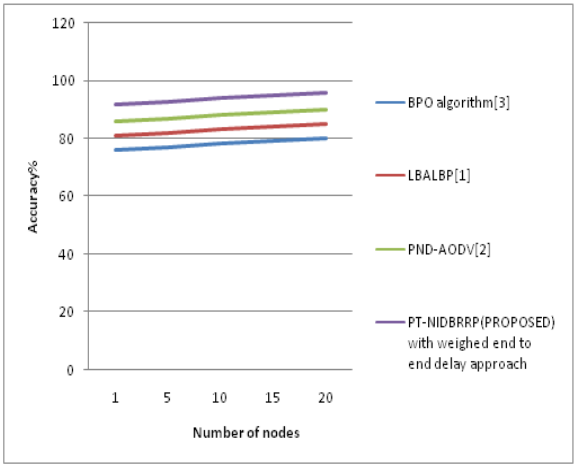

Fig.11. Number of nodes Vs. accuracy

The figure 11 represents the accuracy of the proposed method. The proposed method can acquires higher accuracy when compared to the other existing methods. Because the attack type can be predicted accurately. Here the attack determined is the passive DoS attack which was very hard to predict but by the implementation of the probability distribution method. From the obtained results it was concluded that the proposed novel approach was very efficient in link break and shortest route prediction.

VI. CONCLUSION

The link breakage in the route will lead to the increase in the amount of the packet loss in MANET. Due to this, the Quality of Service (QoS) will be decreased to some extent which in turn makes the challenging issue. To overcome the issue, the proficient trusted node ID based route reservation protocol with weighed end to end delay approach was implemented. The link break mechanism was integrated in the protocol which can also maintain the route efficiently. Here the node receives the data packets and check whether the link breakage is present or not. When it predicts whether there is a break present or else the link can going to break means after word it again chose another path and check whether the link break is present or not. This process can continues until it can get a short and link break lack path. Then after getting the right route it can send a information packets to the destination in a single attempt. Here, the passive Denial of Service (DoS) attack has been determined. Finally, the simulation results shows that the proposed novel protocol can outperforms well in terms of packet delivery ratio, delay, throughput, accuracy, overhead and number of link breakages which will prove the efficiency of the method.

REFERENCES

1. Mandeep Kaur Gulati , Monika Sachdeva , and Krishan Kumar , Load Balanced and Link Break Prediction Routing Protocol for Mobile Ad Hoc Networks, Journal of Communications Vol. 12, No. 6, June 2017
2. Ranjan, N., & Nithya, B. (2018). Potential Node Detection for Route Discovery in Mobile Ad hoc Networks. Lecture Notes in Networks and Systems, 377–388. doi:10.1007/978-981-13-2324-9_38
3. Pal, A., Dutta, P., Chakrabarti, A., Singh, J. P., & Sadhu, S. (2019). Biogeographic-Based Temporal Prediction of Link Stability in Mobile Ad Hoc Networks. Wireless Personal Communications. doi:10.1007/s11277-018-6016-7
4. Bandyopadhyay, S., & Karforma, S. (2019). Securing Packet Transmission Through Trusted Shortest Network Path Using Fuzzy Forecasting for Mobility of MANET Nodes. In Security, Privacy and Trust in the IoT Environment (pp. 255-288). Springer, Cham.
5. Robinson, Y. H., Krishnan, R. S., Julie, E. G., Kumar, R., & Thong, P. H. (2019). Neighbor Knowledge-based Rebroadcast algorithm for minimizing the routing overhead in Mobile Ad-hoc Networks. Ad Hoc Networks, 93, 101896.
6. Pandey, P., & Singh, R. (2019). Approaches for Enhancing the Performance of Routing Protocols in MANET. Available at SSRN 3351023.
7. Robinson, Y. H., Balaji, S., & Julie, E. G. (2019). PSOBLAP: Particle Swarm Optimization-Based Bandwidth and Link Availability Prediction Algorithm for Multipath Routing in Mobile Ad Hoc Networks. Wireless Personal Communications, 106(4), 2261-2289.
8. Amiri-Doomari, S., Mirjalily, G., & Abouei, J. (2019). Stability-based routing, link scheduling and channel assignment in cognitive radio mobile ad-hoc networks. Wireless Networks, 25(4), 2013-2026.
9. Mahalakshmi, S., & Vadivel,(2019) R. Dynamic Shrink Route Optimization (DSRO) Technique For Preventing Link Breakage In MANET. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 09
10. Fatima, M., Bandopadhyay, T. K., & Gupta, R. (2019). Unconventional Prediction Algorithm for Quick Route Convergence and Stability in MANET. In Computing, Communication and Signal Processing (pp. 409-418). Springer, Singapore.
11. Prakasi, O. G., & Varalakshmi, P. (2019). Decision Tree Based Routing Protocol (DTRP) for Reliable Path in MANET. Wireless Personal Communications, 1-14.
12. Calarany, C., & Manoharan, R. (2019). An Efficient Evaluation of Bi-Objective Optimization of Path Stability Model for Mobile Ad Hoc Networks Using EN2RP. Journal of Computational and Theoretical Nanoscience, 16(4), 1454-1464.
13. Khanna, G., Chaturvedi, S. K., & Soh, S. (2019). Reliability evaluation of mobile ad hoc networks by considering link expiration time and border time. International Journal of System Assurance Engineering and Management, 10(3), 399-415.
14. Kumar, J., & Kathirvel, A. (2019). Analysis and Ideas for Improved Routing in MANET.
15. Kumar, K. P., & Babu, B. P. (2019, April). A Simple and Cost-Effective Anomaly Detection Paradigm on the Basis of Computational Intelligence for Mobile Ad-Hoc Networks from a Security Viewpoint. In Computer Science On-line Conference (pp. 78-86). Springer, Cham.
16. Sharma, V., Alam, B., & Doja, M. N. (2019). An Improvement in DSR Routing Protocol of MANETs Using ANFIS. In Applications of Artificial Intelligence Techniques in Engineering (pp. 569-576). Springer, Singapore.
17. Kanellopoulos, D. N. (2019). Recent Progress on QoS Scheduling for Mobile Ad Hoc Networks. Journal of Organizational and End User Computing (JOEUC), 31(3), 37-66.
18. Waheed, A., Wahid, A., & Shah, M. A. (2019, May). LAOD: Link Aware on Demand Routing in Flying Ad-Hoc Networks. In 2019 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-5). IEEE.
19. Robinson, Y. H., Julie, E. G., Saravanan, K., Kumar, R., Abdel-Basset, M., & Thong, P. H. (2019). Link-Disjoint Multipath Routing for Network Traffic Overload Handling in Mobile Ad-hoc Networks. IEEE Access.
20. Naresh, M., Raje, A., & Varsha, K. (2019, March). Link Prediction Algorithm for Efficient Routing in VANETs. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1156-1161). IEEE.
21. Sahu, R., Sharma, S., & Rizvi,2019 M. A. ZBLE: Zone Based Leader Election Energy Constrained AOMDV Routing Protocol. International Journal of Computer Networks and Applications (IJCNA).

22. Baskar,M, Gnanasekaran, T & Arulananth,TS,2015, ' IP Based Adaptive Intrusion Tracing Mechanism for Detecting Low Rate DDoS Attacks' International Journal of Applied Engineering Research,Vol.No. 10, No.20, PP 2025-2030

AUTHORS PROFILE

G.Jegan received B.Tech Degree (2008), M.Tech. Degree (2012) and P.hD (2018) in the Department of Electronics and Communication Engineering at pondichery University. He also worked as Project Fellow under the UGC-India supported major research project in Department of Electronics Engineering, Pondicherry University. He has 5 years of teaching experience and currently worked as Associate Professor in the Department of Electronics and Communication Engineering at MLR Institute of Technology, Hyderabad. His areas of interests include Wireless Sensor networks & security, Image Processing.

D.Kamalakannan received B.E., degree in ECE, M.Tech., in Bio-medical Instrumentation and Ph.D in ECE from Anna University, Chennai. He has 23 years of teaching experience. His area of interests include Wireless Communication & Networks, Image Processing and Embedded System

P.Samundiswary received the B.Tech. degree (1997), M.Tech. degree (2003) and Ph.D. (2011)in the Department of Electronics and Communication Engineering from Pondicherry Engineering College affiliated to Pondicherry University, India. She has nearly 18 years of teaching experience. She is currently working as Assistant Professor in the Department of Electronics Engineering of School of Engineering and Technology at Pondicherry University. Her research interests include Wireless Communication and Wireless Networks and Digital Circuit Design using Verilog HDL.