Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Optimization Of Enhanced Link Quality For Ad-Hoc Networks

Dr. Sharmistha Roy[1] , Mr. Devesh Kumar Upadhyay[2] , Sharma Sonu Kumar[3]

[1]Associate Professor Computing And Information Technology Usha Martin University, Ranchi, Jharkhand

[2]Faculty Associate Computing And Information Technology Usha Martin University, Ranchi, Jharkhand

[3]Assistant Professor, Computer Science, Mangalayatan University, Beswan, Uttar Pradesh

ABSTRACT

QoS can't be guaranteed in wireless mobile ad-hoc networks because topology changes so often. Instead, this research proposes a dynamic multipath routing protocol that may automatically pick the best path for different types of data traffic based on current conditions. With multiple-path measurements and weighed cost functions, bandwidth estimates, and DDET counts, various kinds of traffic may get the QoS they need. According to the simulation findings, the new approach is capable of attaining better round-trip speeds and packet delivery ratios than the current protocols. This research has proven that multipath metrics choices may be utilised to boost throughput and minimise end-to-end latency in mobile ad-hoc networks.

KEYWORDS: Round trip time; Wireless mobile ad-hoc network; Data-driven expected transmission; Multipath-metric routing protocol; Quality of service; Packet delivery ratio.

INTRODUCTION

ad hoc networks are self-contained nodes in a wireless network (Corson et al., 1996). There is a virtual link between nodes in an ad hoc network. As soon as the nodes of an ad-hoc organisation begin to communicate, a network is instantly formed. Each node in the network communicates with each other using radio waves. Because there isn't a central AP or base station, the network's nodes may talk to each other. The term "ad hoc network" refers to a local area network that connects automatically to other network nodes (Frodigh et al., 2000).

A wireless network's design may be divided into two categories: infrastructure, which connects the nodes to a central location and peer-to-peer, which allows them to communicate with one another directly. There are nodes communicating with each other over AP as a consequence of this result (Fig. 1). Examples of these networks are GSM, UMTS, and WLAN. Infrastructure-less means that there's no physical representation of the node being communicated with (Frodigh et al., 2000). ad hoc networks are constructed by linking individual terminals together as part of a multi-hop distributed architecture (Stojmenovic and Lin, 2000). Because there is no centralised structure, the ad hoc network's nodes operate as routers (Fig. 2). Ad hoc networks don't have a single point of failure since they aren't static.

LITERATURE REVIEW

CONGLIN RAN, SHUAILING YAN (2021) The topology of an ad hoc network is dynamic and decentralized. Since the nodes can move around freely, routing security has been a challenge that has slowed down development. As a result, a block chain-based multi-path QoS routing security approach (AODV-MQS) has been presented. It is first necessary for the network to set up a chain of nodes, and the states of each node along the chain are saved using intermediate nodes. If nodes do not match QoS requirements, then a smart contract in a block chain is set to reject them. When it comes to smart contracts, a main and standby communication line is identified in the block chain network through smart contracts, which are unrelated to each other. The suggested method performs better than other algorithms, especially in a dangerous setting, according to simulations.

MOHAMMED ABDULHAKIM (2021) Mobile nodes with wireless transceivers form the backbone of an ad hoc wireless network. A temporary structure is needed since it does not rely on any pre-existing infrastructure. Wireless transceivers are used to exchange information between mobile nodes of the network; when information is not in range, other intermediary nodes can be utilized to relay the information in order for communication. With this article, you can gain a broad grasp of wireless ad-hoc network systems and their routing protocols at a macro level, and you'll have access to a wealth of related studies. First of all, this is the first time that Ad Hoc Networks have been discussed in depth with comparisons and simulation tools.

KHALID A. ALATTAS (2021) Congestion is mostly caused by a lack of resources in the mobile ad hoc network architecture. The TCP-based congestion control mechanism, on the other hand, is incapable of controlling and handling the major features of the shared wireless channel system. In the process of understanding the processes of congestion on a thorough basis, it influences the design of suitable protocols and protocol stacks. Even when compared to TCP systems, mobile ad-hoc networks appear to be more difficult to work in. The ad hoc network systems are designed to avoid any form of congestion; hence an agent-based mobile approach for congestion is being developed.

CHI TRUNG NGOA, HOON OHA,(2014) The minimal overhead and great scalability of this routing protocol make it ideal for use in vehicle ad hoc networks. As a consequence of its pathless routing, it has a substantial advantage in that a node with a packet passes it on to its next-door neighbour, and so on, until it reaches its objective. The neighbours' connection stability is uneven because to the shadowing and fading of signals caused by external factors such as vehicle movements. Additionally, as a part of this study, we provide an improved method for predicting a following hop's connection quality, which incorporates both transmission success rates and forecasts of future vehicle placements. Computer simulations show that the suggested measure is accurate.

D. HELEN* AND D. ARIVAZHAGAN (2014) Expanding the ad hoc network has been a recent trend in wireless and small computing. The ad hoc network is made up of flexible flat forms that can move quickly. Robustness, adaptability, and mobility are all advantages of the system. To maximize performance, ad-hoc networks can analyze the radio propagation environment. For this to work, the network node needs to be able to track its location and have memory to recall its current location. There is no hierarchy of devices in an ad hoc network, and each one is free to join any other device within connection range. IEEE802. Wireless networks' ad hoc method of operation is frequently referred to as a "ad hoc network." Ad hoc networks will be examined in terms of their uses, benefits, and drawbacks in this review.

THE MULTIPATH-METRIC ROUTING PROTOCOL

According to the protocol design, route cost would be estimated using multipath metrics. Multiple paths from a source to a destination node may be determined using a weighted cost function depending on data traffic needs.

3.1. Cost Function Design for Multipath-Metrics

By using several path-metrics to estimate the cost, a quick and precise description of the weighted cost function design has been provided here. There were three key variables taken into account: bandwidth, the number of DDETs, and the length of the end-to-end path. The overall cost of a unit path is then determined from the expenses of those measures. In addition, many routes of high quality can be achieved by selecting from a large number of measures for a single route. While different types of data traffic necessitate different kinds of services, multi-quality pathways are more likely to be able to handle all of the traffic. As a result, the total cost of a route is estimated by summing the weighted sums of various cost functions.

$$C_i = \alpha p(u_i) + \beta q(v_i) + \gamma s(x_i)$$

Ci is the total cost of the paths I and. p(u), q(v), and s(x) are cost functions specific to each metric, while N represents the collection of all potential paths leading from a given source and ending at a particular set of destinations. The following is a definition of the cost functions using and as weights for those functions, respectively:

$$p(u) = \frac{u_{\max} - u}{u_{\max}}, 0 \le u \le u_{\max}$$

$$q(v) = \frac{v - v_{\min}}{v_{\max} - v_{\min}}, v_{\min} \le v \le v_{\max}$$

$$s(x) = \frac{x - x_{\min}}{x_{\max} - x_{\min}}, x_{\min} \le x \le x_{\max}$$

There are two ways to describe the DDET bandwidth and the number of route hops: u and v. The values of and are chosen in line with the amount of data that is required. Consequently, depending on the source and destination, a same stream of data might travel more than one path.

$u_{\max}$ is the maximum channel bandwidth, and P (u) in Eq. (2) gives the route cost in terms of bandwidth availability. In Eq. (2), the available bandwidth p increases as the bandwidth cost decreases. Cost of path length v is estimated in Eq. (3) using q(v) and discussed in Section 3 of the paper. In Eq. (3), the smaller the cost, the shorter the path length must be. This fact is also highlighted. This indicates that all the cost functions are in the same range of [0, 1] and that the lower the DDT, the less expensive the route is.

In order to prioritise measurements, a weight for each function is added, with the weighted values altering depending on traffic demands. Weighted value of must be larger than and in order to calculate the route's cost. When it comes to speech data, the importance of should be elevated above that of A shorter and more reliable route has become necessary because of the demands of voice communication. The same is true for data that is more critical than and necessitates even more traffic. Shorter routes cost less because DDET and reliable path selection are improved with a larger weight value.

DDET Design

Experiments were carried out to determine the loss ratio of ad-hoc network links based on the percentage of packets delivered in pairs. In the application layer, we looked at the 802.11b wireless network's physical layer and the CBR standard for data transmission. As shown in Fig. 1, each link is responsible for delivering a specific number of packets. I) a large number of links (which are not likely to transmit data packets) have a high loss ratio, and ii) the delivery ratio for data and ACK packets is much greater than the data and ACK packets. As a result, it's possible that the data and ACK packets don't accurately reflect the link's actual state.

Packet retransmissions are counted as part of the expected transmission count (ETX). All forward and reverse delivery ratios estimated using dedicated broadcast probe packets were used to determine how much ETX was used on each link in a particular routing path.

Since probe packets are so short, the percentage of probe packets sent may not be able to account for link transmission or retransmission. If a high percentage of probe packets are delivered, the probability of packets being dropped is extremely low, even though the link is observed to be lossy. DDET protocol estimates can now be made with more precision according to the methodology described in this work. A link is considered to have no data traffic while measuring the DDET only if probe packets are sent when no data traffic is presented data, or the link's packet delivery ratio, is calculated by each node periodically by monitoring the network's data traffic.

$$d_{data}(t) = \frac{N_{ack}(t-T,t)}{N_{data}(t-T,t)}$$

The node's Ndata(t- T, t) and Nack(t- T, t) values represent the number of packets it sent and the number of acknowledgements it received within time frame T.

The DDET can only be determined from a probing packet if the network is idle at the time of measurement. The probe packet is a sequence of "Hello" packets sent by each host in the network during a predefined time period T. The total number of packets sent and received during this period T is then tallied. dvoice is the ratio of "Hello" packets delivered at t seconds if every mobile terminal sends one at a specific size:

$$d_{hello}(t) = \frac{N_{hello}(t-T,t)}{\frac{T}{\tau}}$$

Assume that T is the total number of received "Hello" packets during the last T seconds, and then divide that number by Nvoice (t-T, t).

A rough estimation of data transfer would be as follows: It's (d)-1 if you're looking at DDET.

For packets of type d, the route's forward delivery percentage is This implies that when data and "Hello" packets are taken into account, d becomes d data(t) and d voice(t) of the route.

df is the likelihood that a forward packet will be successfully delivered at the receiving end when the ETX is calculated using forward and reverse delivery ratios. Herein is found a definition for the probability of packet delivery ratio (dr). Df dr is the probability that a packet will be successfully sent and received. According to Equation (8), the number of transmissions required to successfully acknowledge a failed packet may be estimated by conducting a Bernoulli experiment.

$$ETX = \frac{1}{d_f \times d_r}$$

ANALYSIS OF NETWORKS WITH MOBILE NODES

The nodes' movements were simulated using RWP in the simulation model. In reality, the node's speed is determined at random (0, vmax), with vmax being the fastest possible nodal speed. It is clear from the graphs that protocol performance is better than node speed fluctuation even while maintaining identical data connections.

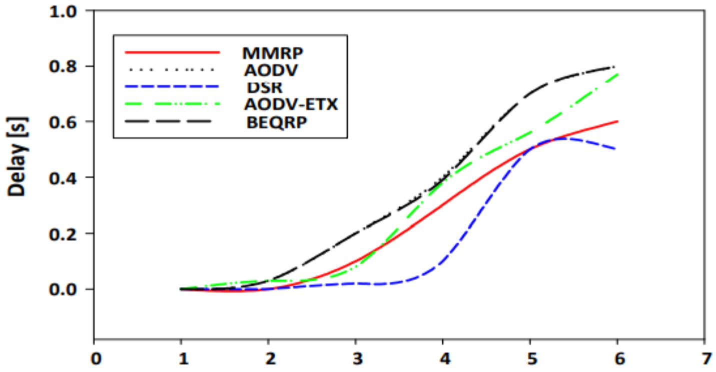

Fig. 1 "Effects of video traffic on end-to-end delay"

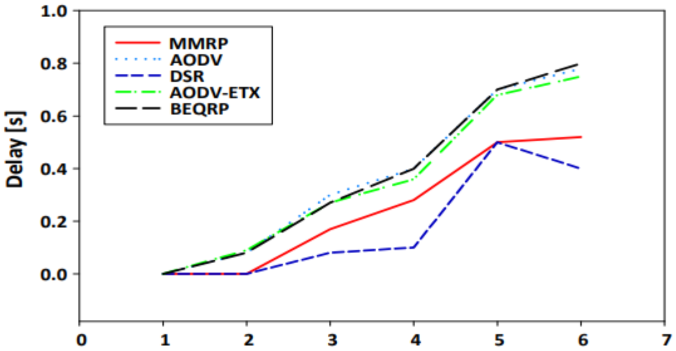

Fig. 2 "Effects of voice traffic on end-to-end delay."

Figure 1 shows that MMRP has a significantly higher PDR than other procedures. Fig. 1 depicts voice traffic's PDR. In this example, MMRP performs best in every situation. It is clear that MMRP selects the most efficient route. The duplicate schemes in AODV, ETX-AODV, and BEQRP are also presented here. In Fig. 1, the PDR data shows that packet data rates fall as the node speeds increase. The MMRP protocol, on the other hand, shows better performance due to a reduced frequency of MMRP route breaks. Protocol-induced connection breakage, illustrated in Figure 2, is causing an impending delay due to nodes' mobility. MMRP, on the other hand, has a lower delay than AODV, ETXAODV, and BEQRP. When compared to other protocols, MMRP has minimal latency, which causes AODV and BEQRP to have a bigger delay. The chart illustrates that AODV, ETX-AODV, and BEQRP all have higher latency than MMRP when it comes to data transmission. Link failures in AODV, BEQRP, and ETX-AODV are to blame for this.

CONCLUSIONS

Cost function model was designed to predict bandwidth, DDET, and route length from the source to the destination to compute the link's cost. When compared to conventional routing protocols, the new technique provides a much better packet delivery ratio and latency. DSR maintains a high packet delivery fraction while altering the speed and pause time for lesser networks. On-demand protocols allow for fewer packets to be discarded because there is always the possibility of a new and active route being picked. On the other hand, because of the increased frequency of link failures caused by on-demand route discovery, the network experiences an increase in routing packets and an increase in end-to-end delay. The NRL and latency are both increased as speed is increased, which in turn leads to more packet drops.

REFERENCE

1. Conglin Ran, Shuailing Yan(2021),” An improved AODV routing security algorithm based on blockchain technology in ad hoc network,” Ran et al. J Wireless Com Network (2021) 2021:52 https://doi.org/10.1186/s13638-021-01938-y

2. Mohammed Abdulhakim(2021),” Moving Ad Hoc Networks—A Comparative Study,” 2021, 13, 6187. https://doi.org/10.3390/su13116187

3. Khalid A. Alattas(2021),” A Novel Method for Avoiding Congestion in a Mobile Ad Hoc Network for Maintaining Service Quality in a Network,” CSNS International Journal of Computer Science and Network Security, VOL.21 No.9, September 2021

4. Chi Trung Ngoa , Hoon Oha, (2014),” A Link Quality Prediction Metric for Location based Routing Protocols under Shadowing and Fading Effects in Vehicular Ad Hoc Networks,” nternational Symposium on Emerging Inter-networks, Communication and Mobility (EICM-2014)

5. D. Helen* and D. Arivazhagan(2014),” Applications, Advantages and Challenges of Ad Hoc Networks,” Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 8 January 2014

6. A. Pal, P. Dutta, A. Chakrabarti, An efcient load balanced stable multi-path routing for mobile ad-hoc network. Microsyst. Technol. 2020(1), 101–112 (2020)

7. 2. A.M. Shantaf, S. Kurnaz, A.H. Mohammed, Performance evaluation of three mobile ad-hoc network routing protocolsin different environments. 2020 International Congress on Human–Computer Interaction, Optimization and Robotic applications (HORA), pp. 1–6 (2020)

8. 3. K. Lei, Q. Zhang, J. Lou, B. Bai, K. Xu, Securing ICN-based UAV ad hoc networks with blockchain. IEEE Commun. Mag. 57(6), 26–32 (2019)

9. 4. A.S. Al Hasan, M.S. Hossain, M. Atiquzzaman, Security threats in vehicular ad hoc networks. In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 404–411 (2016)

10. 5. N. Nishanth, A. Mujeeb, Modeling and detection of fooding-based denial-of-service attack in wireless ad hocnetwork using Bayesian inference. IEEE Syst. J. 2020(3), 1–10 (2020)

11. 6. F. Abdel-Fattah, K.A. Farhan, F.H. Al-Tarawneh, F. AlTamimi, Security challenges and attacks in dynamic mobile ad hocnetworks MANETs. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 28–33 (2019)

12. 7. W. Wei, H. Song, H. Wang, X. Fan, Research and simulation of queue management algorithms in ad hoc network sunder DDoS attack. IEEE Access 5(1), 27810–27817 (2017)

13. 8. M. Karthigha, L. Latha, K. Sripriyan, A comprehensive survey of routing attacks in wireless mobile ad hoc networks. In2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, pp. 396–402 (2020)

14. 9. J. Tang, A. Liu, Z. Jian, N. Xiong, Z. Zeng, W. Tian, A trust-based secure routing scheme using the traceback approachfor energy-harvesting wireless sensor networks. Sensors 18(3), 751 (2018)

15. 10. T. Poongodi, M.S. Khan, R. Patan, A.H. Gandomi, B. Balusamy, Robust defense scheme against selective drop attack inwireless ad hoc networks. IEEE Access 7(1), 18409–18419 (2019)