International Journal of Grid and Distributed Computing
Vol. 11, No. 10 (2018), pp.51-64
http://dx.doi.org/10.14257/ijgdc.2018.11.10.05

Congestion Aware Routing Protocol for Low Power and Lossy Networks

Abheyjeet Singh Chahal[1], Deepti Gupta[2] and Ravreet Kaur[3]

[1,2,3]UIET, Panjab University, Chandigarh, India
[1]chahalabheyjeet@yahoo.com, [2]deepti_gupta49@yahoo.co.in,
[3]ravreet@yahoo.com

Abstract

Network congestion is an emerging issue which degrades the performance of the network and this further leads to a delay in the delivery of packets from source to destination. Backpressure algorithm is commonly used for providing optimal throughput in scheduling and routing decisions for multi-hop networks with the help of changing traffic. All nodes obey the algorithm rules for the exchange of information. But such an assumption does not always hold in realistic scenarios. In this paper we propose a novel mechanism, for prioritizing emergency and regular packets using Event Aware Backpressure Scheduling scheme with multi-level priority approach. For the protection of backpressure algorithm (based on routing and scheduling protocols) against various insider threats, virtual trust queuing is used. The mechanism overcomes the problem of network congestion and delivers the packets from source to destination on the priority basis. Experimental results show improvement in throughput, loss ratio, delay time, network lifetime, protocol efficiency, dropped node, source frequency rates, and destination frequency rates.

Keywords: *Congestion, Routing protocols, Backpressure Scheduling*

1. Introduction

The growing population results in an increase in demands, as new technology is currently adopted by almost every individual and industry. The Internet of Things(IoT) is most widely used in all the fields but due to the amount of network scaling packet delivery leads to network congestion [1]. Network congestion is the major issue that mostly occurs during packet delivery from source to destination in sensor networks. As there exists a number of packets, there may be emergency packets that need to be delivered in a required timeline. Due to the high load on the network, it becomes difficult to deliver emergency packets. There are many existing backpressure scheduling algorithms and more techniques to tackle network congestion and emergency packets but still lacks behind in terms of the throughput of the network. Event Aware Backpressure Scheduling (EABS) algorithm overcomes the problem of emergency packets using backpressure scheduling scheme with the shortest path so that delay time e can be reduced and network congestion can be less. Various parameters are considered for the performance evaluation such as end-to-end delay, forwarding percentage, network lifetime, loss ratio etc. Athes the scheme solves the issue the of emergency packets but still, there are regular packets in the network which needs to be delivered to the destination by a defined time [2].

User data is split into a small amount of information. This small amount of information is called a packet. The source provides a unique number for each

Received (April 25, 2018), Review Result (July 24, 2018), Accepted (August 31, 2018)

ISSN: 2005-4262 IJGDC

packet. These packets are encoded using the base64 algorithm. Source creates a block used to transmit a packet. The packets are shuffled and then placed in the blocks so that every block will contain shuffled packets. Source finds all possible paths to reach the destination. Source sends a block to the destination. The source does not send all blocks through the same path. Each block is sent on a different path. The source generates a codeword for all bocks. The original order of packet's unique number is called a codeword. The codeword is sent in a different channel and that channel is used to send only codeword, not a block. All blocks contain out-of-order packets. The destination arranges the packet using the codeword. The destination receives all blocks from the source and these blocks travel in a different channel. Some channel contains more noises so packet loss easily occurs. Some channel contains very less noise so there is no loss of packets. Blocks traveling in noisy channel lose some of the packets that before reaching the destination. The destination will find an error. The destination indicates the source. The source resends a message in low noise path [3].

The paper here deals with the involvement of emergency as well as regular packets by considering packets with different priorities. The study focuses on the processing of packets from source to destination by considering both emergency and regular packets with multi-level priorities. Our main contributions are as follows-

- The paper mainly focuses on reducing the network congestion by implementing the scheduling scheme with the shortest path so that delay time can be reduced, packet loss ratio should be less and also network throughput can be increased.
- Emergency, as well as regular packets, will be delivered from source to destination using a multi-level priority mechanism. The packets must be prioritized based on the access need.
- Whenever an emergency occurs, the emergency packets will be sensed by the sensor and generate the packets. Each packet's header contains emergency flag and deadline (time to left). The emergency flag indicates whether an emergency has occurred or not and deadline indicates how long data will be available. If the emergency flag is true, that packet is an emergency packet. The packet is inserted in the source queue and the source gives first priority to transmit the data. If the source queue contains more than one emergency packets, then emergency packets are given priority based on the deadline.
- The multi-level priority is based on the dynamic multilevel priority (DMP) packet scheduling algorithm with event aware backpressure scheduling.

The rest of the paper is organized as – Section 1 comprises of Introduction to network congestion and existing scheduling schemes. Section 2 consists of existing Event Aware Back Scheduling (EABS) algorithm. Section 3 is composed of related work, Section 4 is composed of Proposed study. Section 5 consists of Experimental results and comparison whereas Section 6 illustrates Conclusion of the research study.

2. Event Aware Backpressure Scheduling Scheme

The sensor senses the data from the environment and generates a packet. The packets are to be transmitted to the destination. Emergency packets which need to be delivered to the destination in some particular time are generated only when an urgent event occurs. To solve this problem the scheduling scheme is designed. Many

scheduling schemes are available for the sensor networks, such as Collection Tree, ZigBee *etc*. However, these schemes do not guarantee the throughput of networks. In EABS, they implemented a backpressure based scheduling scheme, which can efficaciously control the network congestion. The emergency packet is firstly forwarded, which reduces the waiting delay in queue for an emergency event. Furthermore, the backpressure scheme for emergency packets is combined with the shortest path[2].

In the existing system, a number of packets can cause the problem of network congestion. This situation creates a problem for regular packets in emergency time. The packets are not able to reach the destination by its deadline. Emergency packets take a more time to reach the destination. To solve this problem a scheduling scheme named as EABS is designed and implemented.

2.1. Network Formation

In this module, network formation is done. They consist of a multi-hop network that contains a number of nodes. Each node has some range. The node can communicate within its range. If the range of one node intersects with another node then it defines that both are neighbors. One node can have any number of neighbors. The destination is not a neighbor of the source and it can't send information directly to the destination. It sends a information to its neighbor and the neighbor send a information to another neighbor and then finally it reaches its destination. Source find a path to reach destination [4].

2.2. Backpressure Scheduling

Each node maintains a queue for data transmission. The node sends a packet to another node based on the backlog. Backlog means how many packets are received by the node or available space of the node. The source needs to transmit a data to another node, it first source check the neighbor node how many spaces are available and then transmits the packet. This technique reduces the congestion and increases the throughput [9].

2.3. Emergency Packet Transmission

The emergency packet is transmitted over the internet. Most of the packets are regular packets and that are inserted into the source queue. Source sense the emergency packets and it inserts them into the queue. But a source has some regular packets and these regular packets are transmitted to the destination via the path. The emergency packets should reach the destination before the deadline (time to left). The source transmits the emergency packet to the neighbor which is nearest to the destination. So it selects the shortest path to reach the destination and reduce the transmit time.

The scheme enhances the real-time performance of emergency packets and also reduces the transmission time, delay time and other parameters. But the scheme only focuses on the emergency and regular packets, it does not consider the multi-level priority of packets. The proposed study overcomes this limitation as it introduces the event aware backpressure scheduling scheme with multi-level priority scheme for prioritizing the packets covering emergency and regular packets [10].

3. Related Work

Ala Al-Fuqaha *et al.*, [1] in the paper entitled "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications" Showcase various challenges in the field of IoT, such as availability, reliability, mobility, performance, management,

scalability and interoperability. An overview of IoT enabling technologies, protocols, and applications was provided through the survey. Further, it provides the overview of some key IoT challenges. In this paper, the relation between the IoT and other emerging technologies including big data analytics and cloud and fog computing has been explored.

Tie Qiu *et al.*, [2] in the paper entitled "EABS: an Event-Aware Backpressure Scheduling Scheme for Emergency Internet of Things" proposed an event-aware backpressure scheduling scheme to enhance the real-time performance of emergency packets for EIoT and designed a backpressure-based queue model according to the arrival process of different packets that reduces the waiting time of emergency packets in queues. In the study, only the existence of emergency packets and regular packets was considered. However, packets with different priorities can exist in the network.

Asma Lahbib *et al.*, [3] in the paper entitled "Link reliable and Trust-aware RPL routing protocol for the Internet of Things" proposed a Trust management scheme for securing the network routing topology construction and maintenance within the RPL routing protocol. Trust model was applied to the RPL protocol, evaluated and compared with ETX based MRHOF objective function. Performance of the model in case of other types of attack scenarios; *i.e.*, the attacks targeting the RPL network traffic as well as the network nodes resources is not considered.

Xiyuan Liu *et al.*, [4] in the paper entitled "REMI: A Reliable and Secure Multicast Routing Protocol for IoT Networks" proposed a cluster-based multicast routing protocol for Low-power and Lossy Networks to address the disadvantages of BMRF protocol such as high end-to-end delay, low robustness against single point of failures, and low scalability, at the expense of a slightly higher energy and memory consumption. From the security point of view, there is a need to embed algorithms to counter measure more specific (such as a rank attack) as well as general (such as Sybil) attacks on routing protocols in IoT networks.

Zhenfei Wang *et al.*, [5] in the paper entitled "Energy balancing RPL protocol with multipath for wireless sensor networks" proposed a routing measurement mode—lifecycle index LCI with consideration of link quality, node energy, energy consumption rate, throughput, data transmission speed, congestion detection factor CF (N) and the index finds the bottleneck of candidate path in advance. Work is about to be done on the optimization of the parent node selection scheme; reasonable threshold to reduce the sending of control information in the local repair algorithm using social welfare function; enhance the protocol support for mobility and others.

Arvind Kamble *et al.*, [6] in the paper entitled "Security Attacks and Secure Routing Protocols in the RPL-based Internet of Things: Survey" presented a survey for the classification of the attacks against the RPL protocol in three categories: attacks against network lifetime, network convergence, and network traffic. There is a requirement of the universal solution that is applicable to all the routing attacks.

Tie Qiu *et al.*, [7] in the paper entitled "A Lifetime-Enhanced Data Collecting Scheme for the Internet of Things" proposed an energy-aware and distance-aware backpressure data collecting scheme (EDA) based on the LIFO queue model for the network service chain. There is a requirement to work on the congestion control strategy and dealing with emergency packets while making routing decisions.

Ankita A. Chipde *et al.*, [8] in the paper entitled "A Dynamic Packet Scheduling Scheme with Multilevel Priority for Wireless Sensor Network" proposed a dynamic multilevel priority (DMP) packet scheduling algorithm to overcome the short comes like starvation of real-time data, end-to-end or data transmission delay, and to make the packet scheduling dynamic. It further needs an improvement in assigning priority to a data packet that is based on task deadline instead of shortest processing time and also an improvement in processing overhead by removing data packets with an expired deadline from the medium.

Manu Elappila *et al.*, [9] in the paper entitled "Survivable Path Routing in WSN for IoT applications" proposed a congestion and interference aware energy efficient routing technique that worked in the networks with high traffic because multiple sources try to send their packets to a destination at the same time, which is a typical scenario in IoT applications for remote healthcare monitoring. There is a need to extend the protocol with mac layer designs with transmission power control schemes and traffic adaptive dynamic contention window to have a cross-layer design.

Yang Liu *et al.*, [10] in the paper entitled "Multiple layer design for mass data transmission against channel congestion in IoT" proposed a multiple layer design to solve serial problems about mass data transmission in IoT, specific from architecture, data, protocol, and spectrum layers. Overabundant parameters will increase the computational cost; whereas insufficient parameters may make the essential information deficient.

4. Proposed Approach

A technique is proposed for transmission over a communication medium that makes use of an unconventional channel of packet order. The order of packets which are to be sent over the network at sender-side is manipulated and the phenomenon is emulated. Interceptors or monitors will not able to order these packets due to the large computational cost of buffering and packet sorting at network core so it is difficult to detect the presence of reordering which is based on a covert channel by monitoring at the network core. A huge amount of traffic passes through network core makes it difficult for an adversary to find covert channel from the huge amount of background traffic. The covert channels will not be detected by the adversary if he randomly monitors the observation points. As packet reordering less occurs at adversary point so it is easier for it to detect the presence of covert channels if a monitor is located near to end device. Network traffic is usually difficult to monitor if it occurs at end devices. To compromise some nodes which are near to end devices or for installation of some eavesdropping gadgets near to end devices adversary is required but these tasks are difficult for it to deal with. At the network layer receiver is able to analyze the ordering of packets secretly. Firstly, the presence of a channel will be detected by an adversary which is, however, an expensive task. Transport layer reorders the packets to deliver it to application layer [7].

The existing study mostly comprises to find the safe shortest path for every node. The evacuation paths lead to congestion those results in more evacuation time. This occurs due to a large number of nodes. The nodes are more in number than the safety capacities of evacuation paths. To solve the problem of emergency navigation is also analyzed in the paper using the distributed algorithm. The emergency evacuation problem is converted to existing network flow problem so that user's evacuation time can be minimized.

Dynamic multilevel priority (DMP) packet scheduling algorithm is used with event aware backpressure scheduling. In this, the hierarchy of nodes is created and each node consists of three levels of priority queues. DMP scheme provides better results than the FCFS scheme. The work also focuses on the improvement of assigning priority to a data packet which is based on a task deadline instead of the shortest processing time. Furthermore, processing overhead is also improved by removing data packets with an expired deadline from the medium [8].

Hierarchical relation structure must be transformed into the simpler structure as hierarchical structure results in more complicated structure and in more classes. For simplicity and easier implementation flat relations are preferred at the design level. The flat relation has no identity or functionality as it corresponds to entity-relationship modeling and many object-oriented methods.

4.1. System Features

In a cluster, each monitored component is monitored by *n* sensing nodes and it can communicate with each other. We assign the cluster name to each cluster and each sensing node stores its cluster name. Each cluster can communicate with the help of forwarding sensors. Each sensing nodes can sense the data and forward the data to the forwarding sensors. Then the measured data can be forwarded to the controller with the help of forwarding nodes. Each sensing node stores the check polynomial of other clusters. Data can be validated by using this check polynomial.

En-route Filtering is an energy efficient scheme as the false messages are filtered at intermediate nodes before posing the impact on remaining nodes in the network. The false message (or report) forged by compromised sensor nodes can use a lot of network and computation resources and reduces the lifetime of sensor networks. Therefore, false reports should be filtered at forwarding nodes as quickly as possible by using the secret key.

4.2. Assumptions

A sensor network is assumed as it detects the hazards. If a 'yes' alarm is triggered by the node then it signifies that it is residing in a dangerous area which is depicted using red color node and if it is in a safe area then it will trigger 'no' alarm which is depicted by the grey color node. The wireless communication network is preferred and it is also assumed that communication devices can track the information using wireless signals. Navigation path should be safe which is mostly ignored in existing studies. Two practical definitions for the safe path and safe capacity are considered. According to which a path is safe if the threshold distance between the sensor node and nearest alarming neighbor node is safe. The safe capacity which is depicted as ui is described as the maximum number of the user passing through the sensor nodes (which are on a safe path) safely per unit time. To describe nodes safety capacities two functions such as constant function and linear function are used as a representative function.

4.3. Dynamic Short Path

For directed, undirected or mixed graphs we can define the shortest path problem. The sequence of vertices in an undirected graph, such a path is called the shortest path. It provides a sub-optimal solution which is not the best but is nearest to the best solution [5].

4.4. Objective and Requirements

A base station is used in which scheduling process works in a fully distributed manner. Every user is guided by sensor nodes along the scheduled path. The paths must be safe which are used by the navigation algorithm. All the users should move out of the emergency area in order to avoid congestion. The total evacuation time should be minimized by the navigation algorithm. The evacuation time of a user is the difference between user's exit time and the time at which emergency occur. To lower the cost, sensor nodes are not equipped with GPS and the communication overhead must also be small.

5. Experimental Results

Simulation results are verified for the research study and performance is evaluated in this section. For performing the simulations various software requirements are considered that covers Tcl, C, and C++, Awk, NS 2.35, Linux (OS), Ubuntu 12.04 whereas hardware requirements cover 500GB and Above hard disk, 4GB and Above (RAM) and I3 and below processor. For the simulation of the

proposed protocol, NS (Version 2) is used. In the simulation, the network that is used has an area of 1053x597 with user-defined n number of nodes, packet size is 1024 bytes and the protocol used for routing is DSDV.

5.1. Simulation Model

A simulation model is used that consists of n (user-defined) nodes and n UDP/TCP connections that studies inter-layer interactions and their performance implications. The other parameters used in this model are as under:

Table 1. Parameters used in the Simulation

Software for simulation	Network simulator 2.
Channel	wireless
Simulation runs time	100 seconds
The area in which nodes move	1053X597
Packet size	1024bytes
Speed	1m/s to 10 m/s
Routing Protocol	DSDV
Propagation model	TwoRayGround
Network Interface Type	Wireless Physical
Queue Type	Drop Tail
IFQ-Length	50 Packets
MAC Type	Mac/802.11
Antenna Type	Omni Antenna

Using the packet delivery ratio the performance is analyzed.

5.2. Other Non-functional Requirements-

5.2.1. Performance Requirements

Response time is estimated from the time that the user performs out the activity that says "Go" until the point that the user gets enough response from the PC to proceed with the task. It is the client's subjective holdup time. The response time that is insignificantly satisfactory whatever is left of the time. A more extended response time can make users think that the system is down. You likewise need to indicate rest of the time. Response time degradations can be all the more expensive at a specific time.

5.2.2. Safety Requirements-

The software might be security basic. Provided that this is true, few problems are related to its integrity level. The software may not be well-being basic in spite that it frames some portion of a security basic framework. For instance, programming may essentially log exchanges. In the event that a system must be of a high integrity level and if the software is appeared to be of that integrity level, at that point the hardware must be at any rate of a similar integrity level. There is little point in creating 'idealize' code in some dialect if hardware and software are not reliable. Systems with various requirements for security levels must be separated, otherwise, highest integrity level is applied in the same environment.

Table 2. Representation of Various Test Cases

Module	Test case ID	Input	Expected output	Actual output
Packet size	TC 01	1000	As rate is 1000k, the transmission should begin.	Packet transmission started
Input file (tcl file)	TC 02	.tcl file	After successful execution of the .tcl file,nam file created.	Nam file created as tcl file executed out.nam.
Output file	TC 03	.tcl file	Nam file should be created	Nam file created. Out.nam created
Trace file	TC 04	.tcl file	Graphs must be displayed	.tr files generated and graphs displayed

There are various factors that are considered to evaluate the performance of the proposed study that covers packet loss ratio, throughput time, delay time of packets delivery from source to destination, number of channels utilized to control the congestion of network, source frequency, destination frequency, number of nodes dropped and protocol efficiency is also verified. Figure 1 depicts the packet loss ratio that occurred during the packet transmission from the source to the destination of proposed and existing study. The packet losses are illustrated during various time intervals while the transmission. DORP is based on a medial axis graph giving the emergency areas. In the following, we present the design principles in three steps: constructing the medial axis graph, formulating the navigation schedule problem, and designing the distributed algorithm. The color bar in red represents the existing study of EABS while the green color represents the proposed study. The xgraph format is selected for evaluating the performance of the study. The packet loss of the proposed approach is less as compared to existed EABS.

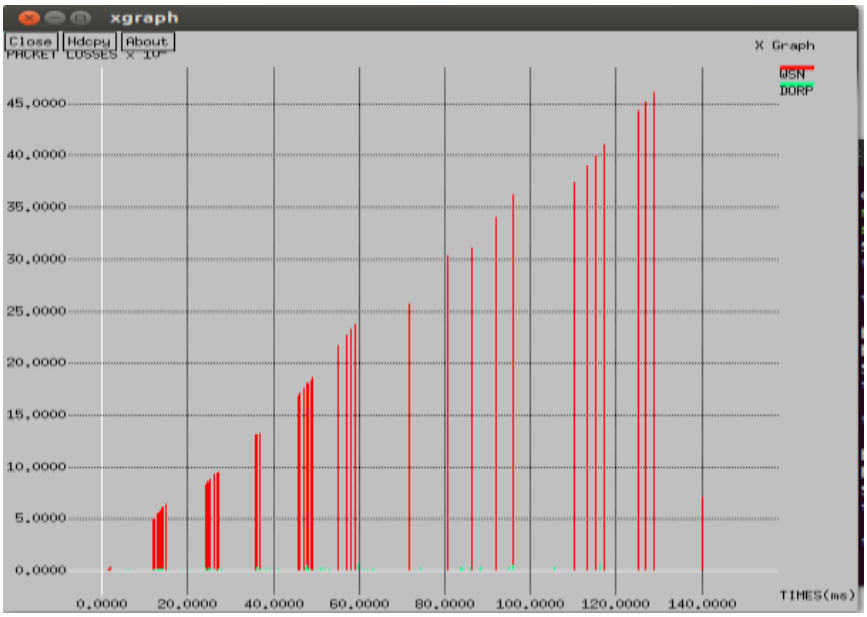

Figure 1. Packet Loss Ratio

The greater number of network channels leads to less network congestion and more network lifetime which helps in easier transmission of packets from source to

destination. If there are less number of channels available in the network then the load increases due to which it becomes difficult to send the data packets. This also gives rise to network congestion. Figure 2 illustrates the channel utilization of the existing and proposed mechanism. The proposed approach makes use of more number of channels to control the traffic and load on the network.

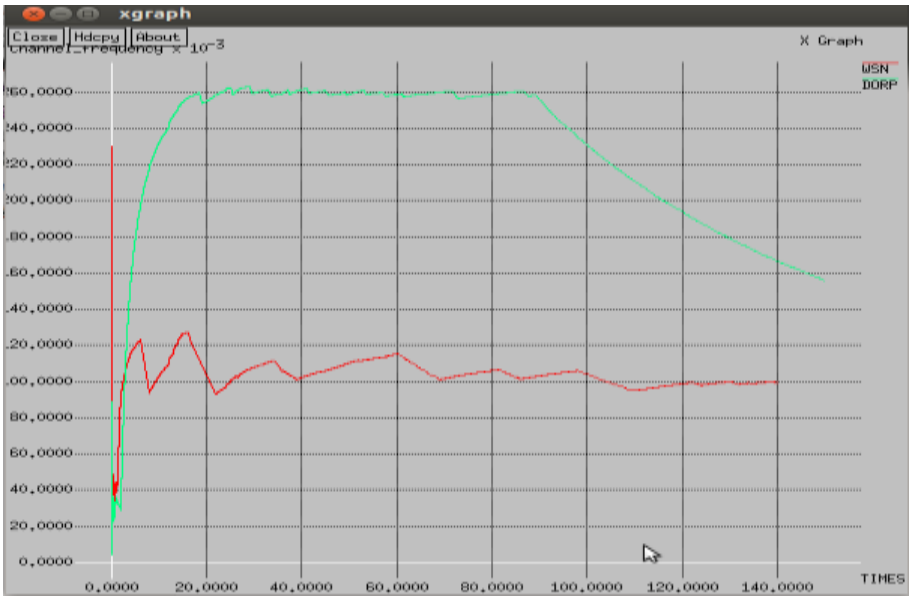

Figure 2. Channel Utilization

Figure 3 shows the delay time during packet transmission, it is defined as the average time from the generation of the packet to its delivery. Delay time is considered as an important factor for evaluating the performance of scheduling mechanisms. It can be seen that with the increase of arrival rate of packets the delay time increases in case of EABS scheme whereas in case of proposed approach the delay time is less as the packets are prioritized and scheduled. While prioritizing the packets the emergency and regular packets both are considered.

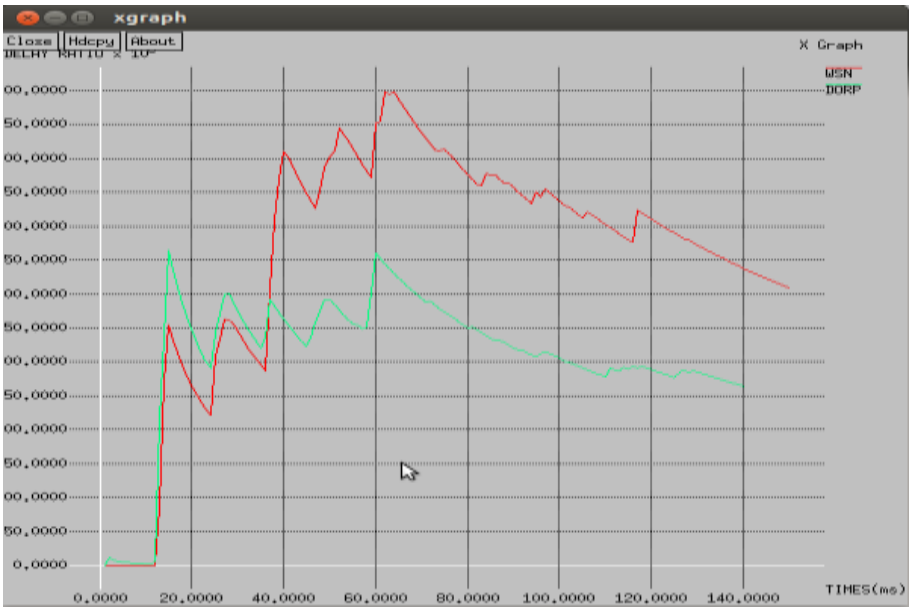

Figure 3. Delay Time

Figure 4 illustrates the destination frequency which signifies that at what frequency rate the packets are received by the destination nodes. Higher is the destination frequency lower will be the network traffic and also load will be lower on the network.

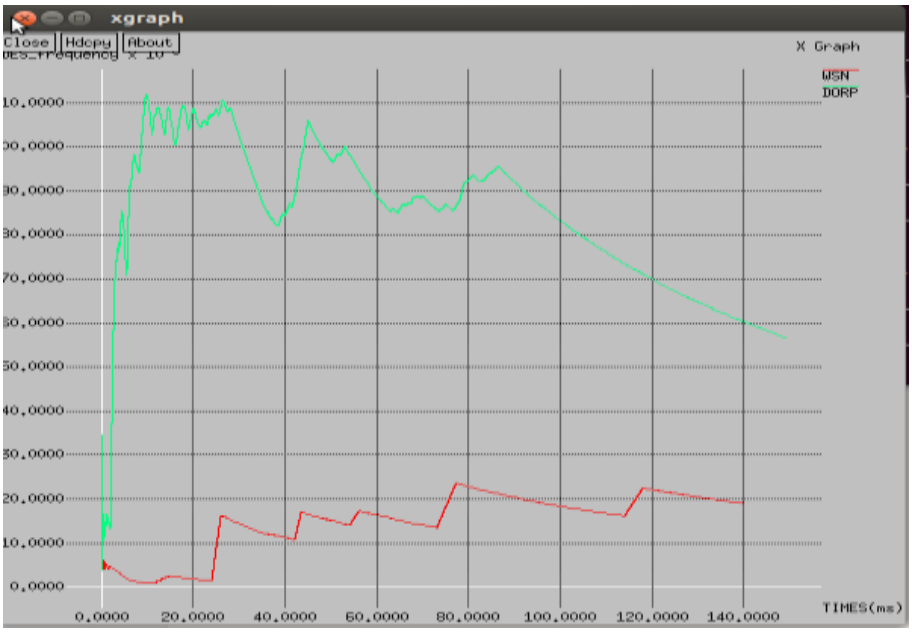

Figure 4. Destination Frequency Rate

During the simulation process, there are many nodes that get dropped due to more energy consumption and less network lifetime. Figure 5 depicts the dropped nodes of existing EABS and proposed approach. The proposed approach has less number of node dropped rate. As discussed in the existing literature that the regular packets consume more energy after delivered at the destination so this drawback is overcome in the proposed study by prioritizing the packets.

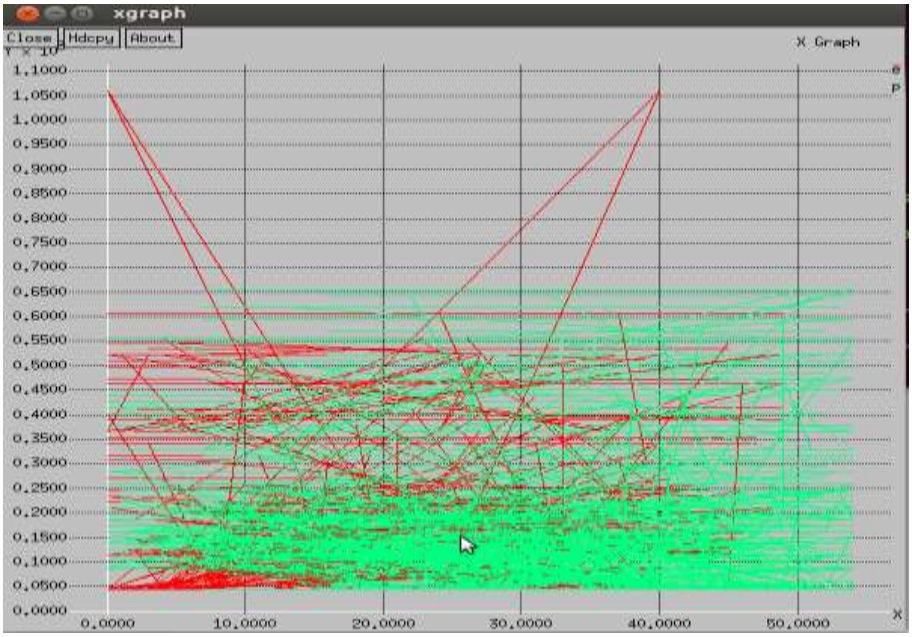

Figure 5. Dropped Nodes

DSDV protocol is used for better efficiency whose simulation results are depicted in Figure 6. With the use of DSDV protocol, the transmission occurs in a smooth and consistent way.

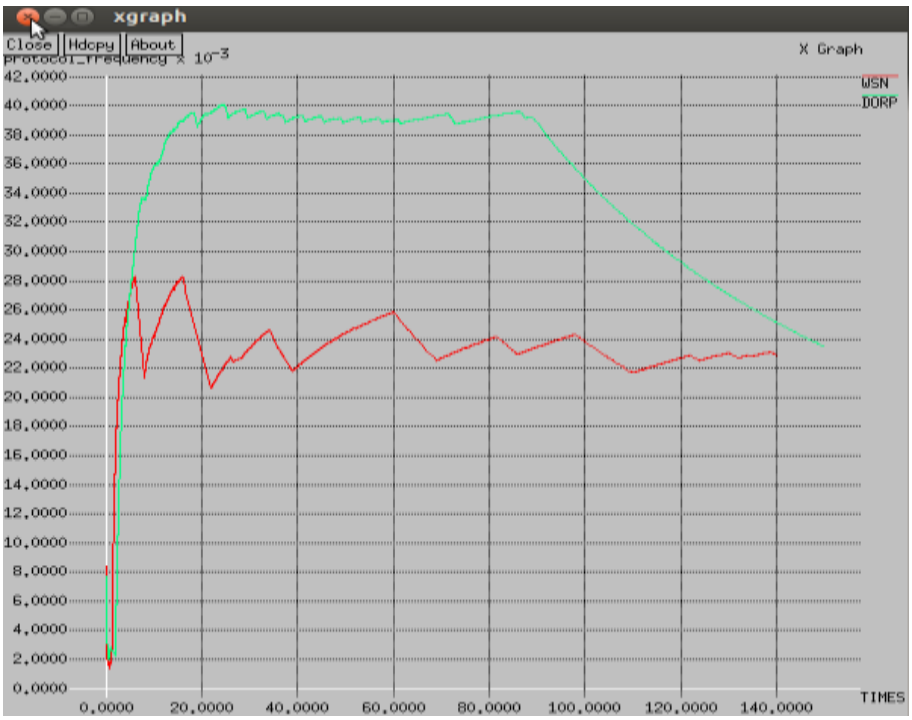

Figure 6. Protocol Efficiency

Figure 7 demonstrates the source frequency graph comparison of existing and proposed approaches. Source frequency signifies the frequency rate of arrival of packets *i.e.*, at what frequency packets start arriving from the source node.

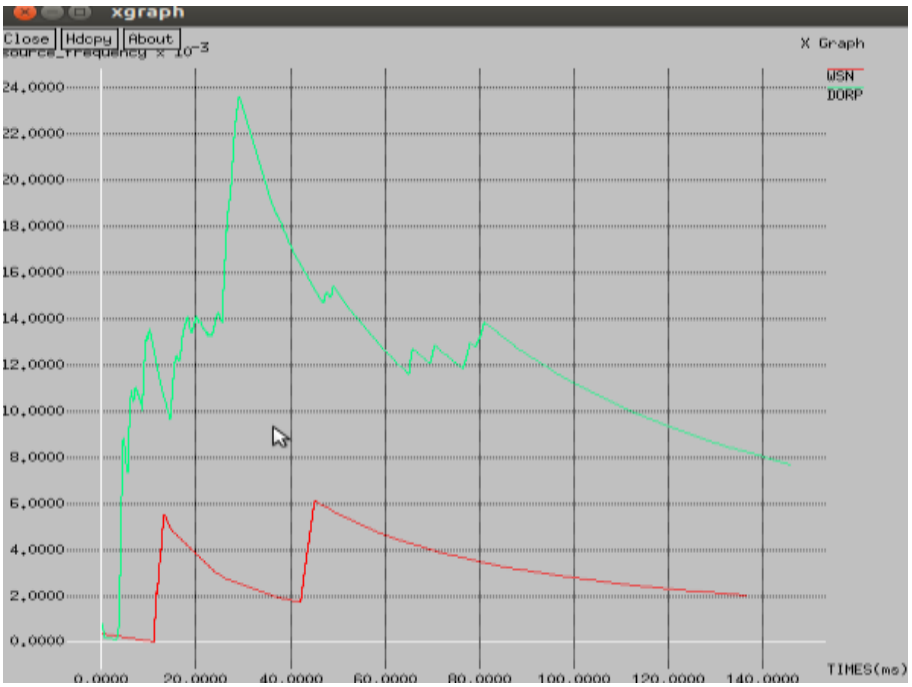

Figure 7. Source Frequency Rate

Throughput defines the successful rate of packet delivery. The proposed approach takes less time for packet transmission whereas the existing scheme takes more time than the proposed approach. Figure 8 depicts the throughput comparison for evaluating the performance.

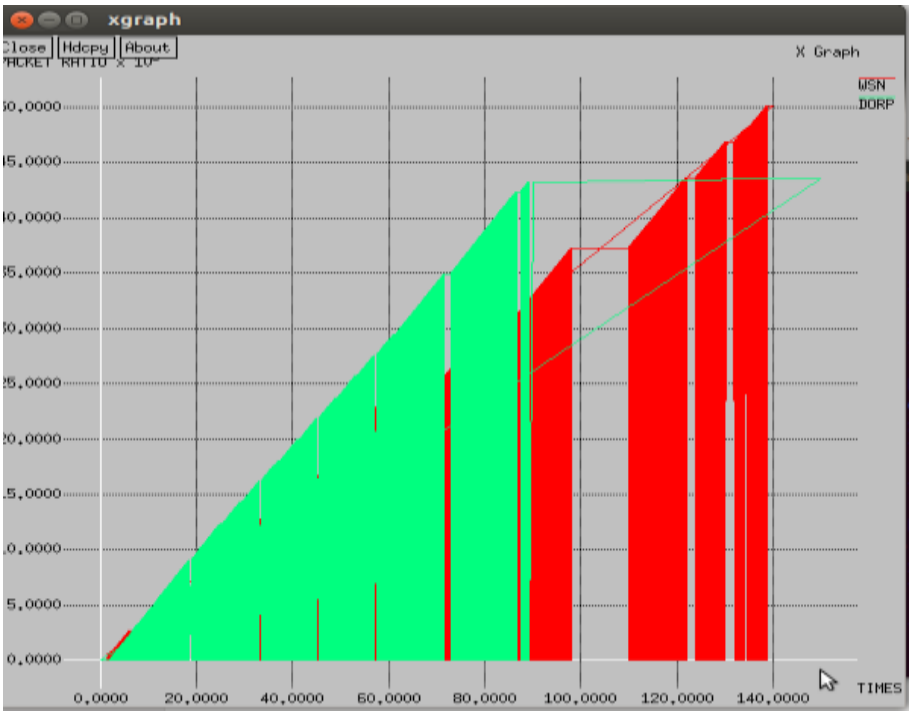

Figure 8. Throughput Time for Packet Transmission

The results justify that the proposed approach outperforms better in terms of delay time, loss ratio, throughput, network lifetime, protocol efficiency and other performance evaluating factors.

6. Conclusion

The paper proposes a safe, ordered, and speedy emergency navigation algorithm. To solve the problem of network congestion, delay time, throughput and also to minimize users' evacuation time, the emergency evacuation problem is converted to a traditional network flow problem. A reliable algorithm *i.e.*, Event aware backpressure scheduling with multi-level priority approach solves the problem of emergency as well as regular packets to deliver packets from source to destination within the mentioned specific time deadline. By assigning the priority to the packets it becomes easier to control the congestion problem on the network. Our simulation results have shown that our scheme is better than the existing approaches in terms of network congestion, throughput, delay time, loss ratio and network overhead and also in terms of many other discussed factors.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications", IEEE Communications Surveys & Tutorials, vol. 17, no. 4, **(2015)**, pp.2347-2376.

[2] T. Qiu, R. Qiao and D. O. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things", IEEE Transactions on Mobile Computing, vol. 17, no. 1, **(2018)**, pp. 72-84.

[3] A. Lahbib, K. Toumi, S. Elleuch, A. Laouiti and S. Martin, "Link reliable and trust aware RPL routing protocol for Internet of Things", Proceedings of IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, US, **(2017)** October 30 - November 1.
[4] M. Conti, P. Kaliyar and C. Lal, "REMI: A Reliable and Secure Multicast Routing Protocol for IoT Networks", Proceedings of the 12th International Conference on Availability, Reliability, and Security, Reggio Calabria, Italy, **(2017)** August 29 - September 01.
[5] Z. Wang, L. Zhang, Z. Zheng and J. Wang, "Energy balancing RPL protocol with multipath for wireless sensor networks", Peer-to-Peer Networking and Applications, vol. 11, no. 5, **(2017)**, pp. 1085-1100.
[6] A. Kamble, V. S. Malemath and D. Patil, "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey", Proceedings of International Conference on Emerging Trends & Innovation in ICT (ICEI), Pune, India, **(2017)** February 3-5.
[7] T. Qiu, R. Qiao, M. Han, A. K. Sangaiah and I. Lee, "A Lifetime-Enhanced Data Collecting Scheme for the Internet of Things", IEEE Communications Magazine, vol. 55, no. 11, **(2017)**, pp. 132-137.
[8] A. A. Chipde and V. G. Kasabegoudar, "A dynamic packet scheduling scheme with multilevel priority for wireless sensor network", International Journal of Computer Applications, vol. 110, no. 10, **(2015)**.
[9] M. Elappila, S. Chinara and D.R. Parhi, "Survivable Path Routing in WSN for IoT applications", Pervasive and Mobile Computing, vol. 43, **(2018)**, pp. 49-63.
[10] Y. Liu, Z. Chen, X. Lv and F. Han, "Multiple layer design for mass data transmission against channel congestion in IoT", International Journal of Communication Systems, vol. 27, no. 8, **(2014)**, pp. 1126-1146.

