Enhancement path assured transfer protocol to transmit urgent data

Abstract: Sensor network is designed to provide monitoring services especially for natural disaster. These natural disasters may affect lives of human beings directly or indirectly. Congestion is a very important factor in wireless sensor network (WSN) and also it reduces quality of services. Different types of data are generated in WSN and sensor nodes also depend on meant factors. It is very important to control the congestion as it may cause loss of packets or even more utilization of energy by sensor nodes. Congestion can be reduced by increasing the number of resources, reducing the transfer from source node or prioritizing the data that has to be sent. The data is categorized into two types, urgent data and normal data. Urgent data or sensitive data should be given more priority than the normal data. The proposed system checks for urgent data and give priority to urgent data, and by this the sensitive data will reach destination in time. In many previous systems, normal data was discarded. In the proposed system, normal data will not be discarded but it will be sent by some other alternative path to the sink node. The result shows better performance.

Keywords: wireless sensor network, urgent data, enhancement path assured transfer protocol, normal data, sink node

8.1 Introduction

Wireless sensor networks (WSN) acquired more attention just because of its varied and attractive applications in numerous fields. WSNs are the wireless networks and having remotely distributed sensors to coordinately observe, monitor and store the environmental conditions or any required information. There are many applications related to WSNs and also it is an integral part of day-to-day life. Monitoring applications depend on WSNs. They are used to monitor pressure, sound, temperature and so on. The applications include target tracking [1], online anomaly detection [2], biometrics and health care [3], wireless body sensor networks in medical applications [4], object tracking [5] and many other useful applications. A WSN consists of huge quantity of sensor nodes and these preprocess the raw data by some easy computations and transmit the essential preprocessed data. A sensor is used to sense, computate and communicate, and it is equipped with a small battery. There are some characteristics of sensor like small size, lightweight and portability that makes WSN as best choice among various applications. The WSN is an advanced technology that helps the society to be more safe,
comfy and secure. WSN as a social infrastructure is capable to transfer critical data very quickly and is more reliable than some other data. WSNs of this type would generally transmit both urgent and normal data. This data should be handled differently as priority of data will be different. The system transmits important data with lower delay and higher reliability related security, environment, disaster or condition monitoring applications. So we can say that WSN is able to categorize critical and noncritical data and give priority to packets based on its importance and urgency depending on the request that comes from the application layer. The objective of this idea is to get awareness of quality-enabled networks for environmental observation and monitoring mainly for calamity avoidance and urgent reply situations.

The real-time communication is one of the challenging problems in WSN. Sensor nodes can transmit very limited, irreversible and power sources because of their ad hoc strategy of deployment and low cost. Thus, a standout among the many constraints is to decrease the energy consumption as less as possible of sensor network. The different WSN applications such as border surveillance must be able to operate for quite a long time without any wired power providers. Along these lines, specifically, the delay requirements of packets must be met at very less energy value in WSN.

WSNs can interact with their environment through different sensors, process the data in sensor node itself as it has simple computation capability, and communicate processed data with all their neighbors. Following components are included in the sensor node:

- Wireless modules are the main constituents of WSN. They have the communication abilities and the memory for programming the application code. A module contains a transceiver, microcontroller, power source, few sensors and programmable memory unit.
- A sensor board that is attached on the wireless module is embedded with many types of sensors. Sensor board contains a prototyping area.
- Programming boards provide many interfaces that connect wireless modules to an enterprise or any PC/laptop or industrial network. The programming boards are used either to program the wireless modules or gather data from wireless modules [6].

There are different types of sensor nodes based on application in which it is used. They have different storage memory size, speeds, transmission rate and operating frequency.

The data packets can be transferred from one node to another by using different transmitting paths that may utilize different times to reach. Many different and alternative paths will be available at different times. Hence, we need the device or protocols that will send data packets in comparatively less time. This path that uses minimum time is called the best path among all available paths. These protocols
are the routing protocols. The disadvantage of these routing protocols is that they ignore the power levels of the nodes in the available minimum time path. By this, nodes may end up sending noncritical or nonurgent data packets repeatedly using all the power of these nodes. Therefore, these nodes will run out of power and come out of WSN. Later data packets need to transmit from different available nodes that may use more time. By this, the critical data may not reach on time to its destination and incur huge loss. It is required to deal with these problems. Normal data and urgent data should be categorized and transmit by different paths. Urgent data only should be transmitted using best path. We proposed an algorithm that will categorize the urgent data from normal data by checking the priority. And then dedicate the best path to the urgent data transmission. Normal data will be transmitted using the alternative paths.

8.1.1 Characteristics in transport protocol design

Characteristics of transport layer protocol are as follows:

- Connection oriented: The Sender and receiver establish the connection before the data transmission begins. When the sender sends the data, it gets the positive/negative per packet response or selective ACK/NACK response from its recipient.
- Same order delivery: When the sender divides the packets into number of fragments by assigning the sequence number to each for transmission, then transport layer protocol transfers packets sequentially to the receiver in the same order as they were at the source node in order to reconstruct it again.
- Reliable data: If all the packets reach the base station (BS) successfully in the same order, then the BS send the selective acknowledgment to sender; otherwise, BS sends the negative acknowledgment to increase the reliability.
- Flow control: If the flow rate of sensor nodes is huge prominent than that of processing rate of receiver node, then congestion happens around the receiver node. To minimize the congestion, the flow rate of sender has to be controlled.
- Congestion detection and avoidance: Network congestion is detected by checking the buffer level and load on channel. At the node level, congestion can be avoided by setting the threshold value to buffer. When it increased more than the threshold of buffer, it sends backpressure message to sender to decrease flow rate in order to solve the congestion. Second issue is: Load on channel; if downstream node does not receive the packet within the pre-defined time, then it assumes that the congestion occurred in the network due to large delay. Solution to this problem is also the same, that is, to adjust the reporting rate of sender, so that the receiver can handle and process the packets.
Loss recovery: It is a very sensitive issue for some applications such as military surveillance and many more. Some application may tolerate the loss of packets such as temperature monitoring. Many researchers have contributed their efforts to achieve the loss recovery with minimum energy expenditure. The cache and noncache techniques allow the transport layer protocol to achieve the loss recovery. Also, the retransmission mechanism is helpful to recover the lost packets by checking the packet numbers.

8.1.2 Issues in transport protocol design

Issues in transport protocol (TP) design are discussed below.

- **Congestion control:** Perform reliable delivery and congestion control of data.
  As large amount of data is transferred from the source node to master node, the congestion may occur around the master node. In spite of the fact that MAC convention can get back the lost packets because of bit error, there is no chance of taking care of packet loss because of buffer exceeding its limit. WSNs require a component for packet loss recovery, for example, acknowledgment and specific acknowledgment utilized in TCP. Moreover, in WSNs reliable delivery may have a different importance in comparison to the long-established networks; accurate transfer has to be ensured. Some sensor applications just need to get data appropriately from a few nodes around the region. It is not important to get data from all nodes in the respective region. This perception may cause a vital contribution in the plan of WSNTP. Likewise, it might progressively be powerful to utilize a level-by-level approach that can control overcrowding and diminish loss of packets, and along these lines it conserves energy. The level-by-level system may likewise bring down buffer necessity at intermediate nodes.

- **Quality of service (QoS):** WSNs sending data protocol ought to make the underlying connection establishment method simpler or go through connectionless protocol to improve the process speed, reduce the transmission delay and enhance throughput. Many applications of WSNs are reactive, so it implies that they monitor passively and trust that occasions will happen before transferring the data to the master node. These types of applications can have several packets to transfer as the outcome of an event.

- **Packet dropping rate:** In order to avoid energy waste, TP in WSNs ought to avoid the packet losses, however, much as could be expected. To avoid this, TP utilizes active congestion control (ACC) to bring down the connection use by some margin. ACC triggers congestion evasion before congestion really happens. For instance, of ACC, intermediate or sender nodes decrease its transfer rate as buffer size of neighboring nodes surpasses up to specific limit.
Throughput: The TCP is supposed to ensure fairness for various nodes all together as every node can accomplish reasonable throughput.

Cross-layer optimization: If feasible, TP ought to be structured with this optimization. For instance, if a routing method tells the TP about failure of route, then the protocol ought to have the capacity to derive that loss in data or packet is from path failure and not because of overcrowding in network. In such a scenario, the sender may continue with its current rate.

Issues of WSN are coverage ability, need of specialized hardware, QoS, security, congestion in network, network connectivity, prolong the network survival time, network expansibility support, algorithm complexity and others [7, 8].

This chapter deals with congestion control in network. The data transmitted can be urgent data or normal data. Urgent data has to be transmitted by giving it the most priority. There are many different protocols that are made only for urgent data transfer. The existing systems mainly focus on urgent data transfer and discard other information. The proposed enhanced path assured transfer (e-PAT) system transmits both urgent and normal data but more priority will be given to the urgent data, and the dedicated path will be assigned for transmission of urgent data [9].

8.1.3 Constraints of WSN

Despite the fact that a large number of protocols have been useful to wireless or wired network, these protocols cannot be utilized to sensor network as they hold unique characteristics that recognize it from different kinds of wireless or wired networks. The attributes are as follows:

- The sensor nodes equipped with short-range radio communication are prone to high latency, high failure rate and limited bandwidth.
- Sensor’s range of transmission is short and mostly impacted by transmission power.
- The sensors are normally equipped with batteries and are supposed to operate unattended for longer time. Therefore, energy consumption is the essential requirement. A sensor acquires more energy on communication rather than computation.
- Sensors have restricted computational ability and have less memory. This restricts the different algorithms and results in processing of a sensor.
- The communication is affected by obstacle or noise.
- There are large numbers of sensor nodes, so they do not contain global ID.
- Due to movement or including more number or failure of sensor nodes changes the WSN topology.
8.1.4 Path-assured protocol for WSN to transfer urgent data

This protocol consists of the following steps:

i) For blocking normal data transfer, the urgent data node starts blocking request to all other nodes. Blocking of data transfer is a help to clear the path.

ii) Here critical or urgent data is transmitted directly to the sink node, and the sink node will give ACK for the received message, then actual data transmission takes place and when it is done the sink node sends the release message for releasing the node. Here data transmission takes place without collision because direct path is generated from source to sink and also by doing so it decreases delay because of retransmission, packet drop.

iii) This technique increases the network lifetime and reduces network overload by simulation

8.1.5 To develop a PDNC method with security for WSN

Selective packet discarding technique is also used in the proposed system. These techniques help congestion control by removing unwanted packets from communication. We also use Remote Control Protocol (RCP) protocol for congestion control in wireless networking. RCP-CA helps to control the traffic by

i) Quality control: Establish a target flow rate, such as Control Packet Rate (CPR).

ii) Acceleration control: it limits the acceleration.

iii) Feedback control: main aim of this is to decrease packet loss occurred during transfer.

Advantages of planned system controlling congestion from WSN using RCP protocol: It increases energy efficiency for discarding congestion control and the results are compared with the PAT and e-PAT based on the performance metrics like energy consumption, packet delivery ratio, delay and packet drop.

8.1.6 A proposed system to transfer urgent and normal data

e-PAT method

Here a number of protocols are designed for data transmission (urgent). In the PAT protocol, the node first asks for urgent data transmission to destination. In that case, the sensor node also stops transfer of normal data so that it sends a blocking request. This will block the transmission of normal data and clear the path; hence, it transmits urgent data very fast and don’t have to wait for data transmission also there is no any fear of collision and packet loss and also avoid congestion in
network and provide 100% reliability for urgent data so here normal packets are
blocked and not sanded in network and which is not stored at node because of
memory shortage. So this is a major issue resolved in the proposed system by using
intelligence. The proposed system is compared with the Packet Discarding Node
Clustering (PDNC), and PAT depends on its performance metrics like energy con-
sumption, packet drop ratio, delay and packet delivery ratio. Hence, the proposed
technique increases the data protection and decreases latency.

The chapter is organized as follows. A brief literature survey on existing sys-
tems is given in Section 8.2. System flow and working of system is explained packet
discarding node clustering in Section 8.3. In Section 8.4, results are discussed.
Section 8.5 concludes.

8.2 Literature survey

Alipio and Tiglao [9] proposed a cache-aware congestion control protocol. They de-
designed a protocol with a mechanism, which is mainly based on management of
cache rules that increase cache consumption. They conducted simulations, and de-
derived method to evaluate the efficiency with occurrence of loss of packets in WSN.

Tao and Yu [10] proposed an enhanced congestion recognition and prevention
system. This system is an energy-efficient control system for WSN. For recognition
of congestion it measures congestion that uses weighted buffer difference and dual
buffer thresholds. Queue scheduler is used to select next packet that has to be sent.
Whenever congestion is caused the packets are selected based on channel loading
and packets urgency.

In WSNs, the capacitor is used to store harvested energy. These capacitors dis-
charge over time or discharge when there is data transmission. To transmit data
only this harvested energy can be used and harvesting of energy requires more
time. Hence, using this mode, transmission of urgent data to sink node is impossi-
ble [12]. The hybrid access point exuded energy to users and the received informa-
tion is transmitted to sink node by using harvested energy by users [13]. By using
backscatter communication system, the users receive sudden excitation energy ra-
diated by the hybrid access point.

Sridevi et al. [14] projected a model based on various traffic in WSN of many
different paths. This protocol assigns bandwidth that is directly proportional to
number of applications running in sensor nodes at the same time. The dataflow will
be forwarded to multiple paths towards destination node.

Wan et al. [16] proposed PSFQ. It is a trustworthy communication from master
node to sensor nodes. Pump Slowly Fetch Quickly (PSFQ) is intended to be energy
efficient and scalable, attempting to limit the quantity of signaling messages and
depending on various local timers. It expects to share out data from the master
node to other sensor hubs by pacing information at a generally moderate rate, yet
permitting hubs that encounter loss in data to bring any lost segments from prompt neighbors forcefully. It consists of three operations: pump, report and fetch. It issues Negative ACK in turn around way to recovering lost fragments. Master node can make sensor hubs to input information conveyance status to it through a basic level-by-level report operation.

Few disadvantages of PSFQ are as follows:
1) It cannot distinguish the single packet loss.
2) It utilizes statically and gradually pumps the outcome in huge wait.
3) Level-by-level recuperation with cache will increasing buffer. To lessen the impacts among these packets, the nodes utilize random delays before replying. At last, to check data delivery status information, the report activity/operation is started by the source.

Wan et al. [16] studied the CODA protocol, which is related to upstream congestion control. It explained energy-efficient congestion control plot with three plans, that is,

i) Open-loop level-by-level backpressure
ii) Congestion detection
iii) Source-to-destination multisource rule

Congestion Detection and Avoidance (CODA) endeavors to distinguish overcrowding by checking the present buffer use and remote channel load. The node identifying overcrowding will tell its next neighboring node about decreasing the transfer speed. The next neighboring hubs will generate to reduce yield speed as that of Additive Increase/Multiplicative Decrease (AIMD). At last, CODA manages multisource rate with the use of closed-loop end-to-end approach as pursued, and as a sensor rate overwhelms the hypothetical throughput, it will set “regulation” bit in even packets. In occurrence the occasion packet obtained by destination has a “regulation” bit. An ACK control note is send by the sink nodes to sensors for informing them to increase their data transfer speed. If overcrowding is reduced, the destination node will effectively mail ACK control note to sensor nodes and to illuminate them to expand their speed. To regulate sensors rate CODA utilizes the mode similar to AIMD in TCP.

It has some disadvantages:
1) Result in decreased reliability, particularly in situations with inadequate source and more data speed
2) Response/delay time required will be expanded under substantial overcrowding

Dipti Patil et al. [17] described the PCCP protocol. It gives congestion control in upstream and fairness. PCCP figures a congestion degree with a solitary measure that is proportional to mean packet arrival time to the mean packet service time. PCCP utilizes implicit overcrowding warning by piggybacking blockage data in header of information parcels. In this manner, maintaining a strategic distance from extra control bundles of Priority-based congestion control protocol (PCCP) utilizes
a bounce by jump rate modification plot called need-based rate alteration, and the three utilizations needs identified with hub need file to arrange traffic are source traffic need, travel traffic need and worldwide need. In any case, in PCCP, the need is characterized from a hub perspective rather than the traffic stream perspective. Along these lines, the traffic streams from a hub can’t be separated.

8.3 Proposed system

The e-PAT protocol is proposed. This protocol transmits both normal and urgent data. In this, the path is dedicated if urgent information is detected and transferred through dedicated path. At the same time, if normal data has to be transmitted then it will be transmitted through alternate path toward sink node. Obviously, priority will be given to urgent data but normal data will not be discarded. Figure 8.1 shows the system flow diagram of e-PAT. First, data will be checked whether it is urgent data. This is checked by the eflag bit in the end device table. If it is an urgent data, then first send a broadcast message to all neighboring nodes and allocate a dedicated path for transfer of that urgent data to the destination node and transfer the data. If it is not an urgent data then it will be the normal data and continue sending normal one. In between if normal data gets detected, then send this data through nodes that are not in the dedicated path. Once urgent data transmission gets over, transmit normal data to the next hop level and then to the sink node.

8.3.1 Proposed system flow diagram

In WSN, urgent data transfer is considered to be very important. The proposed system is e-PAT protocol. There are three steps when end nodes detect the urgent data.
1. It broadcast urgent data detection message to all other neighboring nodes.
2. Once urgent data detection message is received, these nodes stop transmitting normal data and give priority to urgent data and dedicate the specific path to urgent data.
3. The normal data will then be transmitted by using alternate path nodes that are not in the dedicated path for urgent data transmission. Hence, urgent data and normal data will be transmitted by different paths to the next hop toward sink node.
4. As soon as urgent data transmission completes, sink node will be free to accept normal data.

This increases performance of the system.

Some procedure is required to check whether the data is urgent or normal. The system will not know about the type of data it is receiving. It is required to tell the system which one is urgent data. For that, there is one end device table. In this
Figure 8.1: Proposed system flow diagram.
table, 1 bit is eflag bit, that is, emergency flag, and this bit gives the information about urgent data.

### 8.3.2 Enhanced path assured transfer algorithm

e-PAT algorithm is given below. Data or information from different sensor nodes is input for this algorithm. The output is based on the priority of data, that is, whether data to be transmitted is normal or urgent. At the sink node, all data will be received. Priority of urgent or sensitive data is more than that of normal data. Based on priority, data will be received by the destination node.

Algorithm: Enhanced Path Assured Transfer
Input: Data from Sensor network.
Output: Data received by sink node based on priority (urgent or normal data). The priority of urgent data is more than normal data.

```plaintext
{ 
1. If data is urgent data then
   Send block broadcast message to all neighboring nodes.
Else
   Continue sending normal data
2. Create selected path tree for urgent data transmission.
3. If normal data detected then
   Send this normal data through nodes which are not in selected path tree.
Else
   Stop
4. If urgent data transmission complete than
   Transmit normal data
Else go to step 2
}
```

### 8.3.3 Mathematical model enhanced path assured transfer algorithm

Let S be the system.

\[ S = \{D_i, D_o, F\} \]

Where

\[ I/P-D_i = \{d_1, d_2, d_3, .. d_n\} \]

Where \( d_1 \) is data from \( s_1 \)
d2 is data from s2
dn is data from sn
where {s1,s2, . . .,sn} are sensor nodes
O/P-Do={du,dn}
Where du is data (urgent) received by sink node
dn is data (normal) received by sink node
F={PDR,PLR,AD,T}
PDR=packet delivery rate=∑packet received/ time
PLR=packet loss rate=∑sent packet- received packet/time
AD=Average delay =∑(packet received time- packet sent time)/n
T=Throughput=∑packet delivered/ packet received

8.4 Results and analysis

The accompanying measurements are considered during analysis of e-PAT protocol performance.

- Transmission delay: This delay is estimated as an interim between transmissions of data packet from its sensor nodes to the destination of data packet at the destination node:
  Average delay = ∑(packet received time – packet sent time)/n
- Packet delivery ratio: It is proportion of packets received at master hub to the number of packet transmitted. Packet delivery ratio is determined as that of individual sensor node and that of overall network.
- Throughput: Throughput = ∑packet delivered/packet received

Simulation parameter

An e-PAT is implemented in an NS2 simulator environment and a wide-ranging simulation experiment is conducted. In simulation experiments, different sensor hubs are consistently distributed in 500 m × 500 m two-dimensional area with a sink node at the lower point. We occupy a general broadcast-based and unicast-based routing protocol for network layer. In these routing protocols, it is thought that each node knows its distance from the sink node.

To evaluate e-PAT, PDNC and PAT performance, the parameters are measured in two scenarios:
1. Urgent data transfer
2. Normal data transfer

Main attributes used in checking of e-PAT, PDNC and PAT system are interval, node and packet size.
8.4.1 Interval

Figure 8.2(a) gives comparison of PDNC, PAT and proposed e-PAT system based on its interval and packet delivery ratio. Red line denotes less packet delivery ratio as distinguished by the black line. Red line is for PDNC protocol and black line indicates the PAT protocol. And blue line for e-PAT system in that packet dropped is very high when compared with others.

Figure 8.2: A comparative study of PDNC, PAT and e-PAT: (a) interval versus packet delivery ratio and.

Figure 8.2: (b) interval versus packet dropped.
Figure 8.2(b) gives a comparison of PDNC, PAT and the proposed e-PAT system based on interval and packet drop ratio. Red line denotes less packet delivery ratio as distinguished by a black streak. Red line is for PDNC protocol and black line indicates the PAT protocol. And blue line for e-PAT system in that packet dropped is very less (Table 8.1).

Table 8.1: Comparison of PDNC, PAT and e-PAT (packet delivery ratio vs interval).

<table>
<thead>
<tr>
<th>Interval</th>
<th>PDNC (%)</th>
<th>PAT (%)</th>
<th>e-PAT (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.3</td>
<td>40</td>
<td>60</td>
<td>80</td>
</tr>
<tr>
<td>0.4</td>
<td>35</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>0.5</td>
<td>20</td>
<td>40</td>
<td>55</td>
</tr>
<tr>
<td>0.6</td>
<td>17</td>
<td>38</td>
<td>50</td>
</tr>
<tr>
<td>0.7</td>
<td>15</td>
<td>35</td>
<td>48</td>
</tr>
<tr>
<td>0.8</td>
<td>10</td>
<td>33</td>
<td>45</td>
</tr>
</tbody>
</table>

Figure 8.3(a) gives a comparison of PDNC, PAT and proposed e-PAT system based on node and packet delivery ratio (Table 8.2). PAT protocol is shown in black line and PDNC protocol in red line. Red line denotes less packet delivery ratio as distinguished by a black line. And blue line for e-PAT system in that packet dropped is very high as compared to the three whenever we consider a different node scenario: 10, 20, 50, 100 nodes.

8.4.2 Node

Figure 8.3(b) gives a comparison of PDNC, PAT and the proposed e-PAT system based on node and packet drop ratio. PAT protocol is shown in black line and PDNC protocol in red line. Red line denotes less packet drop ratio as compared to black line. And blue line for e-PAT system in that packet dropped is very less as compared to three whenever we consider different node scenario: 10, 20, 50, 100 nodes.
Table 8.2: Comparison of PDNC, PAT and e-PAT (packet delivery ratio versus node).

<table>
<thead>
<tr>
<th>Node</th>
<th>PDNC (%)</th>
<th>PAT (%)</th>
<th>e-PAT (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>42</td>
<td>65</td>
<td>70</td>
</tr>
<tr>
<td>125</td>
<td>36</td>
<td>50</td>
<td>55</td>
</tr>
<tr>
<td>150</td>
<td>30</td>
<td>45</td>
<td>55</td>
</tr>
<tr>
<td>175</td>
<td>17</td>
<td>42</td>
<td>56</td>
</tr>
<tr>
<td>200</td>
<td>15</td>
<td>35</td>
<td>48</td>
</tr>
</tbody>
</table>

Figure 8.3: A comparative study of PDNC, PAT and e-PAT: (a) node versus packet delivery ratio and.

Figure 8.3: (b) node versus packet dropped.
8.4.3 Packet size

Figure 8.4(a) provides the packet size versus packet delivery ratio in PDNC, PAT and proposed e-PAT system. PAT protocol is shown in black line and PDNC protocol in red line. The red line denotes less packet delivery ratio as compared to black line. And blue line for e-PAT system in that packet dropped is very less as compared to the three whenever we consider different packet size (Table 8.3).

**Figure 8.4:** A comparative study of PDNC, PAT and e-PAT: (a) packet size versus packet delivery ratio and.

**Figure 8.4:** (b) packet size versus packet dropped.
Table 8.3: Comparison of PDNC, PAT and e-PAT (packet delivery ratio vs packet size).

<table>
<thead>
<tr>
<th>Packet size</th>
<th>PDNC (%)</th>
<th>PAT (%)</th>
<th>e-PAT (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>42</td>
<td>65</td>
<td>68</td>
</tr>
<tr>
<td>35</td>
<td>38</td>
<td>55</td>
<td>58</td>
</tr>
<tr>
<td>40</td>
<td>36</td>
<td>42</td>
<td>45</td>
</tr>
<tr>
<td>45</td>
<td>20</td>
<td>37</td>
<td>39</td>
</tr>
<tr>
<td>50</td>
<td>18</td>
<td>35</td>
<td>38</td>
</tr>
<tr>
<td>55</td>
<td>15</td>
<td>34</td>
<td>35</td>
</tr>
</tbody>
</table>

Figure 8.4(b) provides the node versus packet drop ratio in PDNC, PAT and proposed e-PAT system. PAT protocol is shown in black line and PDNC protocol in red line. The red line denotes less packet drop ratio as compared to black line. And blue line for e-PAT system in that packet dropped is very high as compared to the three whenever we consider different packet sizes.

8.5 Conclusion

Data is categorized into two types, urgent data and normal data, which will be sent to the sink node. Urgent data or sensitive data should be given more priority than the normal data. In this system, the system checks for urgent data and gives priority to urgent data; by this the sensitive data will reach destination in time. In many previous systems, normal data was discarded. In this proposed enhanced path assured system, normal data will not be discarded but it will be sent by some other alternative path to sink node, or normal data will be sent once the congestion is reduced. Both normal and urgent data will reach the sink node, and more priority is given to urgent data; hence, it reaches first. The result shows better performance and throughput.

References


