CHAPTER 5

QUALITY OF SERVICES BASED DIFFERENTIATION QUOTIENT FOR DATA DELIVERY USING ZONAL NODE AUTHENTICATION MODEL IN WSN

5.1 INTRODUCTION

Wireless sensor network uses the abstained misdirected routing method for avoiding the misdirection of route over various topological structures. The routing misdirection is computed based on the packet flow relation measure and adjusted packet flow relation measure. The abstained misdirected routing uses the Erlang’s C Formula with the help of Poisson process for packet flow relation with arrival rate to avoid misdirected route. Relational quality of service routing attains an improved throughput level on changing mobility of sensor node and sink node in wireless sensor network.

Most of the wireless sensor networks have diverse data traffic with different quality of service requirements. Localized multi-objective quality of service routing protocol for wireless sensor network applications have several types of data traffic. For link quality, memory and computation efficient mechanisms are used. Similarly data traffic for reliability, multi-sink single-path approach was used. Though QoS aware dynamic routing for data integrity was ensured in wireless sensor network, however, QoS service rendering needs authentication for multi-zonal sensor nodes.
Zonal Sensor Node Authentication model is designed by service provisioning mode to render data delivery with better QoS differentiation quotient. Wireless sensor network presents a two complexity algorithm for Zone header selection problem and QoS differentiation quotient with sensor nodes and sink nodes. Zonal Sensor Node Authentication model does not requires any information that regards with the sensor network node sink nodes combination. The zone header selection algorithm initially separates the sensor network based on node authentication and measures zone header-sink node combinations. As the sensor node-sink node combination alternatives increases exponentially, it becomes highly impossible to measure the QoS for every sensor node-sink node combination for a large number of sensor nodes in wireless sensor network. The QoS differentiation quotient algorithm is a totally distributed algorithm and does not require any prior information about the network. Each sink node checks the service provisioning of each sensor nodes and forbids placement in the zones based on the QoS differentiation using bandwidth as a measure to serve in the appropriate zone.

5.2 DYNAMIC ROUTING ALGORITHM FOR DATA DELIVERING WITH QoS AWARE CHECKPOINT IN WSN

With the growth of the popularity of wireless media, the number of available sensor nodes (i.e. users) also increase and the need for Quality of Service (QoS) provisioning became apparent. At the same time, due to the diverse nature of traffic, analyzing and providing different classes of QoS requirements is most important. Jiao Zhang et al. (2015) designed Dynamic Routing for Data Integrity and Delay Differentiated Services along with a multi-path dynamic routing algorithm. It was designed to provide low delay and high data integrity. Lyapunov drift technique is applied to prove the stability of the method. Although, communication overhead is suffered
between network and this increases the transmission delay because of load in
the network.

Paul J. Darby III & Nian-Feng Tzeng (2010) developed Decentralized QoS-Aware Check pointing Arrangement (DCA) in WSN for reducing the transmission delay. A reliability driven hardware was constructed with the objective of providing superior checkpoint arrangements in a global manner. By applying reliability driven model, the mobile host act as stable point in network which is used for storing the data and sends the check pointed data to the neighboring mobile host. Moreover, the reliability driven model also served as the means for data recovery during job execution, aiming at increasing the likelihood that does not support the failure data. Though the method DCA served as a measure for data recovery, the network coverage minimized due to the energy constrained sensor nodes.

5.2.1 Dynamic Routing for Data Integrity and Delay Differentiated Services

The Dynamic Routing for Data Integrity and Delay Differentiated Services developed for solving different transmission delay. This method constructed a virtual hybrid potential field. Based on quality of services, application packets are classified and allocated the weights to each packet, and routes the packets towards the sink through different paths. With this routing path, data reliability was improved for integrity-sensitive applications but at the same time also minimized the end-to-end delay for delay-sensitive applications.

Integrity and delay differentiated routing provides high integrity applications and reduced delay transmission. Whenever, the data packets are sent from source node to the destination, the shortest path for transmitting the packets effectively is identified. Next task in data transmission follows the
transmission of packets effectively. Rate control mechanism is designed for storing the data packet transmission with more efficient and based on the length of data information. While transmitting the data packet with shortest path, delay on packet is reduced.

5.2.1.1 Integrity and delay differentiated routing

Integrity services based on different applications are considered in sensor network for packet transmission from source node to sink node. Initially, each data identifies space for uploading the node with excessive quantity of data. Next, hop-to-hop rate control is implied in sensor network for caching the packet transmission efficiently. Short path algorithm is performed for selecting the shortest path of packet transmission with inferior intensity. This process allows packets from source nodes to sink nodes effectively and when there is an excessive packet transmission, there is no dropping node in network. It caches the data in local nodes. Also, traffic aware mechanism is used for spreading the packets with improved integrity application. Delay differentiated services is implemented for reducing the packet transmission delay, accessing the transmission, packet delay and length of packet transmitted.

5.2.1.2 Integrity and delay differentiated routing algorithm

High-integrity or delay sensitive application transmits the packet with queue node more effectively. In the algorithm, routing function is provided based on each node for constructing the depth value of nodes. Multiple sinks in wireless sensor network performs effectively to identify the shortest path in entire sensor network. Thus, each node requires length of data packet and depth that is used for updating the data interval. Here, maximum update interval and least update interval are most commonly used approach for updating the data message.
5.2.2 Decentralized QoS-Aware Checkpointing Arrangement

Decentralized QoS in mobile grid is presented for checkpoint arrangement. QoS-aware middleware is located in wireless sensor network for reducing the packet transmission delay. The optimal checkpoint consists of less reliability driven that sends the data from source nodes to destination in the network. Grid system in sensor network consists of clustering of data and utilization of mobile hosts. Multiple hosts establish checkpoint arrangement to provide an efficient execution with transferring the packet data. Checkpoint arrangement handles different mobile grids to achieve minimum wireless communication. QoS for different user application specifies the user limits, reliability and probability of data checkpoint. Mobile host for wireless links in sensor network protect the data from accessible checkpoint and reduces the failure occurrence of reliable data. QoS aware checkpoint approach effectively recovers the data transmission and reliable data achieves gain efficiently based on checkpoint arrangement.

5.3 ZONAL SENSOR NODE AUTHENTICATION MODEL FOR DATA DELIVERY IN WSN

A wireless sensor network comprises different zone header types (i.e. differentiated bandwidth). The data delivery rendered with QoS differentiation quotient is described by the service provisioning mode based on the zonal node authentication model. Conventional data delivery model lack the ability for efficiently solving data delivery where all nodes are placed in a single network. They use zonal sensor authenticate model for providing efficient handle of different services and combine with multiple sensor network simultaneously.

The network region is split into logical zones, each zone containing a zone header in charge of sensor nodes moving into that zone. The zone
headers are resource-rich in terms of energy and computation. The zone headers communicate with the sink node and therefore reach the destination node. Let us assume that there are ‘n’ zone headers comprising of a unique ID, represented as ‘ZH_i = ZH_1, ZH_2, ..., ZH_n’. On the other hand, the sensor nodes are highly mobile and therefore move among different zones.

Figure 5.1 Block Diagram of Zone-based Sensor Network
The sensor nodes communicate with the neighbor nodes or zone header, but not directly with the sink node and therefore include many sensor nodes with a unique ID represented as ‘\( SN_1 = SN_1, SN_2, ..., SN_n \)’. Whenever a sensor node enters into the network, the public and private key is provided to the sink node; the sensor node with high power is assumed to be the sink node.

Figure 5.1 represents the block diagram of zone-based sensor network. Many sensor nodes are randomly developed in wireless sensor network and node authentication model is performed. The performed authentication model is followed by network partitioning by evaluating node distance based on QoS partition. With the evaluation of node distance based on QoS differentiation quotient, bandwidth is consumed for each sensor network nodes. Finally, it is used to measure the node requirement according to the service provisioning.

### 5.3.1 Node Authentication for WSN

Designing secure authentication model in wireless sensor networks in order to ensure secure and efficient data delivery to the destination is not an easy task due to the mobility factor. The Zonal Sensor Node Authentication model deploys a Node Authentication for wireless network with the objective of improving the data forwarding rate and therefore the data delivery.

Before deployment, each sensor node ‘\( SN_i \)’ knows the public key ‘\( PK(s) \)’ of the sink node and also its own pair of private and public keys, represented by ‘\( PK(SN), SK(SN) \)’ respectively as given in Equation (5.1).

\[
SN \rightarrow (PK(SN), SK(SN)) \tag{5.1}
\]
In a similar manner, all the sensor nodes in the zone-based network, obtains the pair of private and public keys. Followed by this, the sink node obtains all the pair of private and public keys in the network and is formalized as given in Equation (5.2).

\[ s \to \sum_{i=1}^{n} (PK(SN_i), SK(SN_i)) \]  

(5.2)

These computations are then performed by the sink node and by all the sensor nodes before deployment with the objective of preserving their energy and improve the data delivery rate. As a result, whenever a sensor node requires sending data packets to the destination through the sink node via zone header node, the node authentication is performed. The packet therefore includes the data packets (i.e. actual data) and control packet (source node id, destination node id, zone, public key of the sink node and their public key and the private keys).

The sink node checks the already stored public and private keys of the sensor node with the newly arrived sensor node. If both the keys are same, the newly arrived sensor node is authenticated and proceeds with the data forwarding. On the contrary, if both the keys are different, the newly arrived sensor node is not authenticated and no data forwarding is performed. Once the node authentication is performed data forwarding has to be established. Then, zone-based data forwarding is constructed for Zonal Sensor Node Authentication model.

5.3.2 Zone-Based Data Forwarding in Sensor Network

The QoS of WSN in terms of bandwidth utilized and delay time is highly influenced by the way the sensor nodes are organized. But the efficiency of the network is highly affected by the early departure of the
sensor nodes that are away from the sink node. Zone-based data forwarding in wireless sensor network by partitioning the network is developed to deploy the sensor nodes efficiently in the sensing field, organize them in an effective manner by electing suitable zone headers in the zone.

Partition of the network into zones improves the coverage of the sensor nodes far away from the sink node and therefore improving the QoS (reducing the bandwidth utilization and reducing the delay time). Let us assume that the zone distance is ‘R’, possessing ‘W’ width and ‘H’ height, then the number of horizontal hops ‘HH’ and vertical hops ‘VH’ from source node ‘S’ to the zone header node ‘ZH’ are formulated as given in Equations (5.3) and (5.4) respectively.

$$\text{Horizontal hops} \ 'HH' = \frac{W}{R} \quad (5.3)$$

$$\text{Vertical hops} \ 'VH' = \frac{H}{R} \quad (5.4)$$

During the construction of a zone, to select a zone header node is a very critical issue as the responsibility of the zone header node is to render data delivery. Therefore, the zone header node relatively has higher power than the other sensor nodes in the zone with the objective of improving the network lifetime and is formulated as given in Equation (5.5).

$$ZH_i = \sum_{i=1}^{n} \frac{zopt_i}{SN_i} \quad (5.5)$$

Where ‘ZH_i’ symbolizes the zone header that is obtained by the ratio of optimal number of zones ‘zopt_i’ in the network to the total number of sensor
nodes \( \mathcal{SN}_t \) in the network. The distance-based zone header selection algorithm is given below.

Input: Sensor Nodes \( \mathcal{SN}_1 = \mathcal{SN}_1, \mathcal{SN}_2, \ldots, \mathcal{SN}_n \), Zones \( z_1 = z_1, z_2, \ldots, z_n \), Zone Headers \( ZH_1, ZH_2, \ldots, ZH_n \), Source Node \( S \), Data Packets \( DP_1, DP_2, \ldots, DP_n \), zone distance \( R \), width \( W \), height \( H \)

Output: Improved network lifetime

Step 1: Begin

Step 2: For each Source Node \( S \) and Data Packets \( DP_1 \)

Step 3: Partition the network into zones using (5.3) and (5.4)

Step 4: Obtain the zone header using (5.5)

Step 5: End for

Step 6: End

Figure 5.2 Distance-based Zone Header Selection Algorithm

The Distance-based zone header selection algorithm measures the incoming source nodes and data packets and evaluates the zones by partitioning the network. Hence the decision is based on the horizontal and vertical hops and its ability to improve network lifetime. At this stage, the number of sensor nodes in the network is partitioned based on the distance model. A total of \( n \) zone header is measured through which the data forwarding is performed. Once, the Zone-based Data Forwarding in Sensor Network is established, the next step towards the design of Zonal Sensor Node Authentication model is to describe a service provisioning mode.
5.3.3 Bandwidth-based Service Provisioning Mode

Bandwidth based service provisioning mode is widely known that data packets possess different levels of importance according to the application. Therefore a clear distinction of service differentiation or service provisioning mode is highly required to enable the sensor nodes that possess higher service to send the data packets to the destination node be given much preference than the other sensor nodes in the network. In ZSNA model, the sensor node possessing higher bandwidth accesses the data packets faster or travels at a faster rate than that of the sensor nodes possessing lower bandwidth. Figure 5.3 shows the Bandwidth-based Service Provisioning for wireless sensor network.

![Diagram](image)

where

- Sensor node
- Source node
- Zone header node
- Sink node

**Figure 5.3 Bandwidth-based Service Provisioning**

As shown in Figure 5.3, each zone is partitioned according to the bandwidth utilization of each sensor node. Each zone comprises of sensor nodes and zone header nodes, with the network possessing source node, destination node and sink node. The sink node in the Bandwidth-based...
Service Provisioning is the node possessing maximum power among the sensor nodes in the network and is formulated as given in Equation (5.6).

\[ S = \sum_{i=1}^{n} \text{MAXPOWER} (SN_i) \]  

(5.6)

From the Equation (5.6), ‘S’ symbolizes the sink node that is evaluated on the basis of the sensor nodes that possess the maximum power. Next, power required to forward data (i.e. data packets) depends on the volume of information and the square of distance between the sender node ‘S’ and the receiver node ‘D’. It is obtained by selecting appropriate zone distance to the mean transmission cost and is as given in Equation (5.7).

\[ \text{Mean}_{tc} = \frac{\text{Transmission}_S + \text{Transmission}_D}{\text{Dis}} \]  

(5.7)

Where ‘Transmission_S’ and ‘Transmission_D’ symbolizes the transmission power of the sender and destination node respectively with ‘Dis’ representing the distance. The formulation for distance ‘Dis’ is as given in Equation (5.8).

\[ \text{Dis} = \sqrt{\left(\frac{W^2 + H^2}{2}\right)} \]  

(5.8)

Equation (5.8) shows distance formula, where ‘Dis’ is obtained using the width ‘W’ and height ‘H’ of the network. To meet the QoS requirements of different data flows, the service provisioning mode in ZSNA model uses a QoS differentiation quotient algorithm. The QoS differentiation quotient algorithm introduces the bandwidth level to provide differentiated service to a number of sensor nodes in the network. This algorithm supports
differentiated services for sensor nodes with different bandwidths and provides significant dynamic adaptation to traffic conditions.

It is assumed that the algorithm supports three bandwidth levels (i.e. appropriate zone distance), 1Kbps, 1Mbps and 1Gbps respectively. The algorithm cooperates with the objective of reducing the transmission delay and improves the overall QoS performance in terms of data loss rate. Figure 5.4 shows the QoS differentiation quotient algorithm designed with the objective of reducing the transmission delay between the nodes and therefore reduces the data loss in the network.

Input: Network Size ‘W * H’, Zone distance ‘R’, Bandwidth Available ‘Band_a’, Bandwidth Consumed ‘Band_c’, Sensor Nodes ‘SN_i = SN_1, SN_2, ..., SN_n’, Zones ‘z_i = z_1, z_2, ..., z_n’

Output: Reduced transmission delay and data loss

Step 1: Begin
Step 2: For each Sensor Nodes ‘SN_i’
Step 3: If ‘Band_a’ < ‘Band_c’
Step 4: Let Band = Band_c
Step 5: End if
Step 6: If Band(SN_i) < 1Kbps
Step 7: Assign the corresponding zone ‘z_i’
Step 8: End if
Step 9: If Band(SN_i) > 1Kbps and Band(SN_i) < 1Mbps
Step 10: Assign the corresponding zone ‘z_i’
Step 11: End if
Step 12: If Band(SN_i) > 1Mbps
Step 13: Assign the corresponding zone ‘\(z_i\)’

Step 14: End if

Step 15: End for

Step 16: End

Figure 5.4 QoS Differentiation Quotient Algorithm

In the QoS Differentiation Quotient algorithm, that assigns three bandwidth levels to its respective zones for simulation. The proposed ZSNA model is aimed to assign dynamic and adaptive bandwidths to data flows in consideration with different traffic conditions. This provides a good estimate of the future bandwidth utilization of each sensor node in ZSNA model, thus the bandwidth values can be adjusted according to different circumstances.

5.4 EXPERIMENTAL EVALUATION FROM SIMULATION

ZSNA model performs the experimental evaluation using NS2 simulator. The proposed model was modified to allow the QoS service rendering that needs authentication for multi-zonal sensor nodes. ZSNA model is compared with two different methods namely, Dynamic Routing for Data Integrity and Delay Differentiated Services and Decentralized QoS-Aware Check pointing Arrangement in Wireless Sensor Networks. The proposed model simulation assumes a data packet of 50 bytes long and a control packet of 20 bytes long. The transmission range of 200m is assumed to perform data delivery with each sensor node having initial node energy to be 50J. These simulation parameters and their typical values are summarized in Table 5.1.
The sensor networks in the simulations have ‘n’ sensor nodes randomly deployed to a region of network area ‘W * H’ and ‘S’ sink. The deployment region of ZSNA model comprises of a square shaped region with area size ‘2000m * 2000m’. The ZSNA model uses a constant packet generation rate \( Q \) (1 packet/s) for each sensor node. The network lifetime period ends when initial sensor node in network gets stopped. The transmission delay is defined as the delay time taken by a sensor node to reach the destination via zone headers. Data loss rate as the amount of data loss occurred during data delivery in WSN.

Table 5.1 Simulation Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network area ‘W * H’</td>
<td>2000m * 2000m</td>
</tr>
<tr>
<td>Node density</td>
<td>10, 20, 30, 40, 50, 60, 70</td>
</tr>
<tr>
<td>Transmission range ‘R’</td>
<td>200m</td>
</tr>
<tr>
<td>Data rate</td>
<td>250Kbps</td>
</tr>
<tr>
<td>Data packets</td>
<td>7, 14, 21, 28, 35, 42, 49</td>
</tr>
<tr>
<td>Size of data packets</td>
<td>500Kb</td>
</tr>
<tr>
<td>Simulation runs</td>
<td>7</td>
</tr>
<tr>
<td>Node’s initial energy</td>
<td>50J</td>
</tr>
<tr>
<td>Node speed</td>
<td>0 – 25m/s</td>
</tr>
</tbody>
</table>

The performance of the proposed ZSNA model is measured in the following terms:
i) Network Lifetime

ii) Data Loss Rate

iii) Transmission Delay

5.5 PERFORMANCE ANALYSIS OF ZSNA MODEL

The performance analysis of proposed ZSNA model is compared with two existing methods. The compared existing methods are namely, DR-DIDDS by Jiao Zhang et al. (2015) and DCA by Paul J. Darby III & Nian-Feng Tzeng (2010) in WSN. To evaluate the ZSNA model, the following metrics are used.

5.5.1 Performance Analysis on Network Lifetime

The network lifetime refers to the average number of data packets where a sensor node can transmit and receive the data before consuming initial node energy. This demonstrates the effectiveness of routing protocol in the prolongation of network lifetime. The impact of network lifetime in WSN was calculated using the following Equation (5.9).

\[
NL = (DP (size)_s) - (DP (size)_d)
\] (5.9)

From Equation (5.9), ‘DP (size)$_s$’ and ‘DP (size)$_d$’ stand for the overall size of data packets sent and dropped by the sensor nodes in the network.

Example:

- Proposed ZSNA Model:

  Delay time = (100- 13) = 87KB
- **Existing DR-DIDDS:**
  
  Delay time = (100 - 37) = 63KB

- **Existing DCA:**
  
  Delay time = (100 - 54) = 46KB

Table 5.2 (a) and (b) shows the data and performance result on network lifetime. In the experiment, the data packet size of 100KB to 700KB is transmitted at different time interval and the failure probability of the data packet sizes of the proposed ZSNA model is analyzed with that of the DR-DIDDS and DCA.

**Table 5.2(a) Performance Tabulation on Network Lifetime**

<table>
<thead>
<tr>
<th>Size of Sent Data Packets (KB)</th>
<th>Size of Dropped Data Packets (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZSNA</td>
<td>DR-DIDDS</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td>100</td>
<td>13</td>
</tr>
<tr>
<td>200</td>
<td>37</td>
</tr>
<tr>
<td>300</td>
<td>26</td>
</tr>
<tr>
<td>400</td>
<td>29</td>
</tr>
<tr>
<td>500</td>
<td>15</td>
</tr>
<tr>
<td>600</td>
<td>35</td>
</tr>
<tr>
<td>700</td>
<td>28</td>
</tr>
</tbody>
</table>
Table 5.2 (b) Measure of Performance on Network Lifetime

<table>
<thead>
<tr>
<th>Data Packet Size (KB)</th>
<th>Network Lifetime (KB)</th>
<th>Proposed ZSNA</th>
<th>Existing DR-DIDDS</th>
<th>Existing DCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>87</td>
<td>63</td>
<td>46</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>163</td>
<td>142</td>
<td>115</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>274</td>
<td>248</td>
<td>215</td>
<td></td>
</tr>
<tr>
<td>400</td>
<td>371</td>
<td>354</td>
<td>321</td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>485</td>
<td>467</td>
<td>445</td>
<td></td>
</tr>
<tr>
<td>600</td>
<td>565</td>
<td>542</td>
<td>503</td>
<td></td>
</tr>
<tr>
<td>700</td>
<td>672</td>
<td>642</td>
<td>617</td>
<td></td>
</tr>
</tbody>
</table>

Results are presented for different data packet sizes and the results reported here confirm that with the increase in the data packet size, the network lifetime is also increased.

Figure 5.5 Measure of Performance on Network Lifetime
Figure 5.5 explains the network lifetime with respect to the size of the data packet using proposed ZSNA model and is compared with existing methods including ZSNA model respectively. Each of the sensor nodes with different data packet size in WSN cope with network lifetime can be caused by random networks. In order to facilitate comparison, the statistical static ZSNA model and the existing DR-DIDDS and DCA methods were analyzed in the same environment and at the same time. As shown in Figure 5.5, the proposed ZSNA model is significantly improves the network life time when compared to the existing techniques. This efficient improvement in network lifetime, the proposed ZSNA model utilizes the simple zone-based data forwarding in sensor network partitioning the network with the help of zone distance measure. Therefore, network lifetime is improved in proposed ZSNA model by 11% (By considering 100 KB as Data Packet Size, \((87-63)/63=38\%\)). Similarly, it is calculated till 700KB. Then the average value is calculated as 11% ) when compared to DR-DIDDS method by Jiao Zhang et al. (2015) and improved by 29% (by considering 100 KB as Data Packet Size, \((87-46)/46=89\%\)). Similarly, it is calculated till 700KB. Then the average value is calculated as 29% ) when it is compared to DCA method by Paul J. Darby III & Nian-Feng Tzeng (2010).

5.5.2 Performance Analysis on Data Loss Rate

Data loss rate is an important metrics for WSN and it should have low data loss rate to sustain the network. Data loss rate is measured based on the size of data sent and the data received at a given interval of time.

\[
\text{Data Loss Rate} = D_s(\text{size}) - D_r(\text{size})
\]  

(5.10)

Equation (5.10) is used for evaluating data loss rate, where ‘\(D_s\)’ and ‘\(D_r\)’ stands for the size of data sent and data received in wireless sensor
network. The data loss rate is the amount of data loss occurred during data packet transmission from the source node to the sink node.

Example:

- **Proposed ZSNA Model:**
  
  \[
  \text{Data Loss Rate} = (100 - 82) = 18 \text{ KB}
  \]

- **Existing DR-DIDDS:**
  
  \[
  \text{Data Loss Rate} = (100 - 76) = 24 \text{ KB}
  \]

- **Existing DCA:**
  
  \[
  \text{Data Loss Rate} = (100 - 71) = 29 \text{ KB}
  \]

Table 5.3 (a) and (b) shows the data tabulation and performance result with a comparison of data loss rate based on data packet size and the size of data packet is measured in kilobytes. The performance of all the schemes gets better when size of data packets increases.

**Table 5.3(a) Performance Tabulation on Data Loss Rate**

<table>
<thead>
<tr>
<th>Size of Sent Data Packets (KB)</th>
<th>Size of Received Data Packets (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ZSNA</td>
</tr>
<tr>
<td>100</td>
<td>82</td>
</tr>
<tr>
<td>200</td>
<td>177</td>
</tr>
<tr>
<td>300</td>
<td>274</td>
</tr>
<tr>
<td>400</td>
<td>371</td>
</tr>
<tr>
<td>500</td>
<td>468</td>
</tr>
<tr>
<td>600</td>
<td>565</td>
</tr>
<tr>
<td>700</td>
<td>659</td>
</tr>
</tbody>
</table>
Table 5.3(b) Measure of Performance on Data Loss Rate

<table>
<thead>
<tr>
<th>Data Packet Size (KB)</th>
<th>Data Loss Rate (KB)</th>
<th>Proposed ZSNA</th>
<th>Existing DR-DIDDS</th>
<th>Existing DCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>18</td>
<td>24</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>200</td>
<td>23</td>
<td>28</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>300</td>
<td>26</td>
<td>32</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>400</td>
<td>29</td>
<td>36</td>
<td>41</td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>32</td>
<td>38</td>
<td>43</td>
<td></td>
</tr>
<tr>
<td>600</td>
<td>35</td>
<td>43</td>
<td>47</td>
<td></td>
</tr>
<tr>
<td>700</td>
<td>41</td>
<td>46</td>
<td>51</td>
<td></td>
</tr>
</tbody>
</table>

Comparatively, ZSNA model reduces data loss rate, since it appropriates the zone distance to the mean transmission cost and causes an increase in its performance more than the performance increase in any other methods.

Figure 5.6 Measure of Performance on Data Loss Rate
It is seen from Figure 5.6 that the data loss rate and the data packet size is considered. It is found that the ZSNA model with large amounts of data transmission for a long time, data packets with different sizes were significantly lower than that of the DR-DIDDS and DCA. From the Figure 5.6, it is observed that in the proposed ZSNA model data loss rate is reduced compared to the state-of-the-art methods DR-DIDDS and DCA. This is because each zone is partitioned according to the bandwidth utilization and the node that possesses the maximum power is assigned to the sink node. This node performs the data delivery to the corresponding destination node and the ZSNA model combining zone-based design of sensor networks and bandwidth-based service provisioning. It keeps itself more available to the sensor node and the given effective protection, so as to the system for the low rate of implementation of the data loss.

Therefore, the data loss rate in proposed ZSNA model is reduced by 18% (By considering 100 KB as Data Packet Size, \[\frac{(18-24)}{24\times100} = 25\%\]). Similarly, it is calculated till 700KB. Then the average value is calculated as 18% when compared to existing DR-DIDDS method by Jiao Zhang et al. (2015) and 29% (By considering 100 KB as Data Packet Size, \[\frac{(18-29)}{29\times100} = 37\%\]). Similarly, it is calculated till 700KB. Then the average value is calculated as 29% when compared to existing DCA method by Paul J. Darby III & Nian-Feng Tzeng (2010).

5.5.3 Performance Analysis on Transmission Delay

The performance gain due to zone-based and QoS differentiation quotient approaches is investigated under ZSNA model in terms of the performance of transmission delay. Whenever a source node sends data to the destination, it passes through the zone header and to the sink node, and then finally data reaches the destination node. The transmission delay measures the time taken by each sensor node to reach the destination during data delivery.
Transmission Delay (ms) = \((\text{Expected}_t - \text{Actual}_t) \times \text{Number of packets}\) \hspace{1cm} (5.11)

From Equation (5.11), ‘\(\text{Expected}_t\)’ and ‘\(\text{Actual}_t\)’ represents the expected and actual time for data delivery with respect to the number of packets to be sent during each simulation run. It is measured in terms of millisecond (ms).

Example:

- **Proposed ZSNA Model:**
  
  \[
  \text{Transmission Delay} = [(9.5 \text{ ms} - 5.22 \text{ ms}) \times 7] = 29.96 \text{ ms}
  \]

- **Existing DR-DIDDS:**
  
  \[
  \text{Transmission Delay} = [(11.5 \text{ ms} - 6.46 \text{ ms}) \times 7] = 35.14 \text{ ms}
  \]

- **Existing DCA:**
  
  \[
  \text{Transmission Delay} = [(12.75 \text{ ms} - 6.59 \text{ ms}) \times 7] = 43.12 \text{ ms}
  \]

**Table 5.4 (a) Performance Tabulation on Transmission Delay**

<table>
<thead>
<tr>
<th>Number of packets</th>
<th>Expected Time (ms)</th>
<th>Actual Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ZSNA</td>
<td>DR-DIDDS</td>
</tr>
<tr>
<td>7</td>
<td>9.5</td>
<td>11.5</td>
</tr>
<tr>
<td>14</td>
<td>20.56</td>
<td>22.5</td>
</tr>
<tr>
<td>21</td>
<td>22.63</td>
<td>24.52</td>
</tr>
<tr>
<td>28</td>
<td>25.88</td>
<td>28.65</td>
</tr>
<tr>
<td>35</td>
<td>26.6</td>
<td>30.95</td>
</tr>
<tr>
<td>42</td>
<td>29.5</td>
<td>31.55</td>
</tr>
<tr>
<td>49</td>
<td>31.66</td>
<td>34.2</td>
</tr>
</tbody>
</table>
Table 5.4 (b) Measure of Performance on Transmission Delay

<table>
<thead>
<tr>
<th>Number of packets</th>
<th>Transmission Delay (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proposed ZSNA</td>
</tr>
<tr>
<td>7</td>
<td>29.35</td>
</tr>
<tr>
<td>14</td>
<td>35.32</td>
</tr>
<tr>
<td>21</td>
<td>41.45</td>
</tr>
<tr>
<td>28</td>
<td>48.35</td>
</tr>
<tr>
<td>35</td>
<td>38.19</td>
</tr>
<tr>
<td>42</td>
<td>45.31</td>
</tr>
<tr>
<td>49</td>
<td>51.43</td>
</tr>
</tbody>
</table>

The targeting results of transmission delay using ZSNA model with two state-of-the-art methods is in Table 5.4 (a) and Table 5.4 (b) presents the comparison based on the number of packets sent. The comparison between the conventional data delivery method and the proposed ZSNA model with respect to transmission delay is shown in Figure 5.7. The observed packets increase when the Distance-based zone header selection algorithm tends to partition the network based on the distance and activate the data forwarding through the targeted zone header. This results in the desired data forwarding, providing large savings during data delivery. The model as designed is therefore able to reduce the transmission delay for different packets of varying size.
The QoS differentiation quotient as described by service provisioning mode with optimal strategy results in the reduced transmission delay in ZSNA model. With the application of bandwidth-based service provisioning, discrete zone headers are obtained based on the distance at different time intervals resulting in the reduced transmission delay. With the zone headers selected, the source node sends the packets through the header and then to the sink node reducing the transmission delay, whereas in the conventional models, the data packets passes through all the sensor nodes and thereby increases the transmission delay. This is due to the separation of sensor nodes and zone header, the zone header node performs the data forwarding and sends the results to the sink node in WSN.

Hence, the proposed ZSNA model minimizes the transmission delay by 15% (considering number of packets as 7, \([(29.35-36.14)/36.14*100] =18\%\). Similarly, it is calculated till 49 packets. Then the average value is calculated as 15% when compared to existing DR-DIDDS by Jiao Zhang et al. (2015) and 26% (considering number of packets as 7,
[((29.35-43.14)/ 43.14*100) =32%]. Similarly, it is calculated till 49 packets. Then the average value is calculated as 26% when compared to existing DCA by Paul J. Darby III & Nian-Feng Tzeng (2010).

5.6 SUMMARY

A novel Zonal Sensor Node Authentication model and service provisioning is proposed for wireless sensor networks using QoS differentiation quotient. The key idea of the proposed solution is the Node Authentication-based Service provisioning combined with the advantages of Zone-based Data Forwarding using distance measure. Each node during data delivery adjusts its QoS differentiation quotient to satisfy the bandwidth requirements and improve Network Lifetime across different transmission pairs. The former ensures data forwarding whereas the later ensures Network Lifetime. Simulation results obtained for varied WSN topologies that emphasize the advantages of used QoS scheme for WSN. Experimental evaluation is conducted in terms of sensor Node Density and Packet Size, Network Lifetime, Data Loss Rate and Transmission Delay.