HEURISTIC AND SWARM INTELLIGENCE BASED ROUTING PROTOCOL STACK TO RESOLVE THE HETEROGENEITY ISSUES OF INTERNET OF THINGS

THESIS
Submitted
in fulfilment of the requirements of the degree of

DOCTOR OF PHILOSOPHY

By
Shailja Agnihotri
1510951016

Supervised by
Dr. Ramkumar Ketti Ramachandran
Associate Professor – Research
Chitkara University Research and Innovation Network

May 2019

CHITKARA UNIVERSITY
Department of Computer Science and Engineering

CHITKARA UNIVERSITY
CHANDIGARH-PATIALA NATIONAL HIGHWAY
RAJPURA (PATIALA) PUNJAB-140401 (INDIA)
DECLARATION BY THE STUDENT

I hereby certify that the work which is being presented in this thesis entitled “Heuristic and Swarm Intelligence Based Routing Protocol Stack to Resolve the Heterogeneity Issues of Internet of Things” is for fulfilment of the requirement for the award of Degree of Doctor of Philosophy submitted in the Department of Computer Science and Engineering, Chitkara University, Punjab is an authentic record of my own work carried out under the supervision of Dr. Ramkumar Ketti Ramachandran.

The work has not formed the basis for the award of any other degree or diploma, in this or any other Institution or University. In keeping with the ethical practice in reporting scientific information, due acknowledgements have been made wherever the findings of others have been cited.

(SHAILJA AGNIHOTRI)
This is to certify that the thesis entitled “Heuristic and Swarm Intelligence Based Routing Protocol Stack to Resolve the Heterogeneity Issues of Internet of Things” submitted by Shailja Agnihotri, Regd. No. 1510951016 to the Chitkara University, Punjab in fulfilment for the award of the degree of Doctor of Philosophy is a bona fide record of research work carried out by him/her under my/our supervision. The contents of this thesis, in full or in parts, have not been submitted to any other Institution or University for the award of any degree or diploma.

Dr. Ramkumar Ketti Ramachandran
Associate Professor - Research
ACKNOWLEDGEMENT

I would first like to thank my research guide Dr. Ramkumar Ketti Ramachandran, Associate Professor -Research, CURIN, Chitkara University. Due to his positive approach, guidance and constant support, I have been able to complete my PhD work successfully.

I would also like to thank the experts who were involved in the assessment of this study: Dr. Pankaj Kumar, Professor and Dean PhD Programme, Dr. Surya Narayan Panda, Professor and Director Research, Dr. Sachin Ahuja, Professor and Director Research. Without their guidance, suggestions and comments, it was impossible to come this long way. And also, I would like to thank Ms. Deepika Sharma, Assistant Manager, Office of PhD Programme, for always being positive and supportive.

Special thanks to my spouse, Mr. Abhijit Agnihotri, my father Mr. Sushil Sharma and my mother Mrs. Asha Sharma, who are the pillars of my strength and hard work. They have always shown confidence and trust in me and actually believed in my efforts throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. I am thankful to my children, Anirudh Agnihotri and Aaryan Agnihotri, whose quality childhood time I have filched and spent in bringing up this study. Their co-operation is the maximum. I must express my very profound gratitude to my father-in-law. Mr. K.K. Agnihotri, my mother-in-law, Mrs. Chanderkanta Agnihotri, my brother, Mr. Abhishek Bhardwaj and my best friend Dr. Rina, for providing me with unfailing support and continuous encouragement. Also, I am very thankful to Dr. Liza Nanda who spared her precious time and helped me out in proof reading this dissertation.

I am thankful to the Almighty, for being so kind and giving such beautiful people around and making me what I am and HIS grace has led me to complete this study. And I am thankful to everyone who has helped me in direct or indirect way at every step.

(Shailja Agnihotri)
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure No.</th>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.1</td>
<td>IoT technology stack</td>
<td>4</td>
</tr>
<tr>
<td>Figure 1.2</td>
<td>Application areas of IoT</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2.1</td>
<td>IoT Communication Infrastructure</td>
<td>12</td>
</tr>
<tr>
<td>Figure 2.2</td>
<td>IoT architecture</td>
<td>13</td>
</tr>
<tr>
<td>Figure 2.3</td>
<td>IoT Protocol Stack (a)</td>
<td>14</td>
</tr>
<tr>
<td>Figure 2.4</td>
<td>IoT Protocol Stack (b)</td>
<td>15</td>
</tr>
<tr>
<td>Figure 2.5</td>
<td>Application services interface between applications and devices</td>
<td>17</td>
</tr>
<tr>
<td>Figure 2.6</td>
<td>The 3-Layered IoT architecture</td>
<td>18</td>
</tr>
<tr>
<td>Figure 2.7</td>
<td>The 5-Layered IoT architecture</td>
<td>19</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>Sample IoT network</td>
<td>42</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Bluetooth Packet format and protocol stack</td>
<td>44</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>Wi-Fi Packet format</td>
<td>45</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>Zigbee frame format and protocol stack</td>
<td>45</td>
</tr>
<tr>
<td>Figure 4.5</td>
<td>Calculation of Conversion time in IDRA architecture</td>
<td>46</td>
</tr>
<tr>
<td>Figure 4.6</td>
<td>FANT working for ARAH-IoT</td>
<td>51</td>
</tr>
<tr>
<td>Figure 4.7</td>
<td>BANT working for ARAH-IoT</td>
<td>52</td>
</tr>
<tr>
<td>Figure 5.1</td>
<td>IPv6 Packet</td>
<td>54</td>
</tr>
<tr>
<td>Figure 5.2</td>
<td>FANT working for CARA-IoT</td>
<td>59</td>
</tr>
<tr>
<td>Figure 5.3</td>
<td>BANT working for CARA-IoT</td>
<td>60</td>
</tr>
<tr>
<td>Figure 6.1</td>
<td>IoTRSim Interface</td>
<td>62</td>
</tr>
<tr>
<td>Figure 6.2</td>
<td>Sample IoTRSim Simulation</td>
<td>63</td>
</tr>
<tr>
<td>Figure 6.3</td>
<td>FANT BANT working for ARAH-IoT</td>
<td>64</td>
</tr>
<tr>
<td>Figure 6.4</td>
<td>FANT BANT working for CARA-IoT</td>
<td>65</td>
</tr>
<tr>
<td>Figure 6.5</td>
<td>Log file Route.txt-Sample</td>
<td>67</td>
</tr>
<tr>
<td>Figure 7.1</td>
<td>ACO vs ARAH-IoT (Distance)</td>
<td>70</td>
</tr>
<tr>
<td>Figure 7.2</td>
<td>ACO vs ARAH-IoT (Time Taken)</td>
<td>70</td>
</tr>
<tr>
<td>Figure 7.3</td>
<td>ACO vs ARAH-IoT (Hop-count)</td>
<td>71</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>7.4</td>
<td>ACO vs ARAH-IoT (No. of Conversions)</td>
<td></td>
</tr>
<tr>
<td>7.5</td>
<td>ACO vs CARA-IoT (Distance)</td>
<td></td>
</tr>
<tr>
<td>7.6</td>
<td>ACO vs CARA-IoT (Time Taken)</td>
<td></td>
</tr>
<tr>
<td>7.7</td>
<td>ACO vs CARA-IoT (Packet Delivery Ratio)</td>
<td></td>
</tr>
<tr>
<td>7.8</td>
<td>ACO vs CARA-IoT (Average Speed)</td>
<td></td>
</tr>
<tr>
<td>7.9</td>
<td>IoT Network with 10 nodes</td>
<td></td>
</tr>
<tr>
<td>7.10</td>
<td>CARA-IoT vs ACO on the basis of distance (10 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.11</td>
<td>CARA-IoT vs ACO on the basis of hop count (10 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.12</td>
<td>CARA-IoT vs ACO on the basis of conversion time taken (10 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.13</td>
<td>CARA-IoT vs ACO on the basis of average speed (10 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.14</td>
<td>CARA-IoT vs ACO on the basis of end-to-end delay (10 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.15</td>
<td>CARA-IoT vs ACO on the basis of throughput (10 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.16</td>
<td>CARA-IoT vs ACO on the basis of PDR (10 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.17</td>
<td>IoT network with 15 nodes</td>
<td></td>
</tr>
<tr>
<td>7.18</td>
<td>CARA-IoT vs ACO on the basis of distance (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.19</td>
<td>CARA-IoT vs ACO on the basis of hop count (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.20</td>
<td>CARA-IoT vs ACO on the basis of conversion time taken (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.21</td>
<td>CARA-IoT vs ACO on the basis of average speed (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.22</td>
<td>CARA-IoT vs ACO on the basis of end-to-end delay (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.23</td>
<td>CARA-IoT vs ACO on the basis of throughput (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.24</td>
<td>CARA-IoT vs ACO on the basis of PDR (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.25</td>
<td>IoT network with 20 nodes</td>
<td></td>
</tr>
<tr>
<td>7.26</td>
<td>CARA-IoT vs ACO on the basis of distance (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.27</td>
<td>CARA-IoT vs ACO on the basis of hop count (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>7.28</td>
<td>CARA-IoT vs ACO on the basis of conversion time taken (15 nodes)</td>
<td></td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>7.29</td>
<td>CARA-IoT vs ACO on the basis of end-to-end delay (15 nodes)</td>
<td>84</td>
</tr>
<tr>
<td>7.30</td>
<td>CARA-IoT vs ACO on the basis of throughput (15 nodes)</td>
<td>84</td>
</tr>
<tr>
<td>7.31</td>
<td>CARA-IoT vs ACO on the basis of average speed (15 nodes)</td>
<td>85</td>
</tr>
<tr>
<td>7.32</td>
<td>CARA-IoT vs ACO on the basis of PDR (15 nodes)</td>
<td>85</td>
</tr>
<tr>
<td>7.33</td>
<td>IoT network with 25 nodes</td>
<td>86</td>
</tr>
<tr>
<td>7.34</td>
<td>CARA-IoT vs ACO on the basis of distance (25 nodes)</td>
<td>86</td>
</tr>
<tr>
<td>7.35</td>
<td>CARA-IoT vs ACO on the basis of hop count (25 nodes)</td>
<td>87</td>
</tr>
<tr>
<td>7.36</td>
<td>CARA-IoT vs ACO on the basis of conversion time taken (25 nodes)</td>
<td>87</td>
</tr>
<tr>
<td>7.37</td>
<td>CARA-IoT vs ACO on the basis of average speed (25 nodes)</td>
<td>88</td>
</tr>
<tr>
<td>7.38</td>
<td>CARA-IoT vs ACO on the basis of end-to-end delay (25 nodes)</td>
<td>88</td>
</tr>
<tr>
<td>7.39</td>
<td>CARA-IoT vs ACO on the basis of throughput (25 nodes)</td>
<td>89</td>
</tr>
<tr>
<td>7.40</td>
<td>CARA-IoT vs ACO on the basis of PDR (25 nodes)</td>
<td>89</td>
</tr>
</tbody>
</table>
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table No.</th>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1.1</td>
<td>Current IoT Simulators’ features</td>
<td>10</td>
</tr>
<tr>
<td>Table 3.1</td>
<td>Factors affecting MANET, WSN and IoT</td>
<td>33</td>
</tr>
<tr>
<td>Table 4.1</td>
<td>Differences and Similarities between various communication Technologies</td>
<td>46</td>
</tr>
<tr>
<td>Table 5.1</td>
<td>Acceptable delay limit for different type of content on wireless channel</td>
<td>56</td>
</tr>
<tr>
<td>Table 6.1</td>
<td>Sample Routing Table</td>
<td>65</td>
</tr>
<tr>
<td>Table 7.1</td>
<td>Simulation parameters based on ARAH-IoT</td>
<td>69</td>
</tr>
<tr>
<td>Table 7.2</td>
<td>Simulation parameters based on CARA-IoT</td>
<td>69</td>
</tr>
</tbody>
</table>
LIST OF PUBLICATIONS

Research Paper in Journals

Research Paper in Conferences
## ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACO</td>
<td>Ant Colony Optimization</td>
</tr>
<tr>
<td>ACO-AOMDV</td>
<td>Ant Colony Optimization Ad-hoc On demand multipath distance vector</td>
</tr>
<tr>
<td>AD-ZRP</td>
<td>Ant-based Dynamic Zone Routing Protocol</td>
</tr>
<tr>
<td>AODV</td>
<td>Ad hoc On-Demand Distance Vector</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>ARAH-IoT</td>
<td>Ant Colony Based Routing Algorithm for Heterogeneous IoT</td>
</tr>
<tr>
<td>ARM</td>
<td>Architectural Reference Model</td>
</tr>
<tr>
<td>ARAMA</td>
<td>Ant Routing Algorithm for Mobile Ad hoc networks</td>
</tr>
<tr>
<td>BABR</td>
<td>Basic Ant-Based Routing Algorithm</td>
</tr>
<tr>
<td>BER</td>
<td>Bit Error Ratio</td>
</tr>
<tr>
<td>BEAR</td>
<td>Balanced Energy Aware Routing</td>
</tr>
<tr>
<td>CARA-IoT</td>
<td>Content Aware Routing Algorithm for IoT</td>
</tr>
<tr>
<td>CRRP</td>
<td>Cooperative Relay Routing Protocol</td>
</tr>
<tr>
<td>D2D</td>
<td>Device to Device</td>
</tr>
<tr>
<td>DSR</td>
<td>Dynamic Source Routing</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>EAR</td>
<td>Energy Aware Routing</td>
</tr>
<tr>
<td>EEABR</td>
<td>Energy Efficient Ant Based Routing</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hoping Spread Spectrum</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communication</td>
</tr>
<tr>
<td>IABR</td>
<td>Improved Ant-Based Routing Algorithm</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IoT-A</td>
<td>Internet of Things Architecture</td>
</tr>
<tr>
<td>IoMT</td>
<td>Internet of Multimedia Things</td>
</tr>
<tr>
<td>IoTRSIm</td>
<td>Internet of Things Routing Simulator</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>6LoWPAN</td>
<td>IPv6 over Low-Power Wireless Personal Area Networks</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>LLNs</td>
<td>Low Power Lossy Networks</td>
</tr>
<tr>
<td>LPER</td>
<td>Link Packet Error Rate</td>
</tr>
<tr>
<td>MANET</td>
<td>Mobile Ad Hoc Network</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine to Machine</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>OLSR</td>
<td>Optimized Link State Routing</td>
</tr>
<tr>
<td>PDR</td>
<td>Packet Delivery Ratio</td>
</tr>
<tr>
<td>PERA</td>
<td>Probabilistic Emergent Routing Algorithm</td>
</tr>
<tr>
<td>PoG</td>
<td>Probability of Goodness</td>
</tr>
<tr>
<td>PoGoM</td>
<td>Probability of Goodness of Movement</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
<tr>
<td>RT</td>
<td>Routing Table</td>
</tr>
<tr>
<td>SINR</td>
<td>Signal to Interference and Noise Ratio</td>
</tr>
<tr>
<td>SNR</td>
<td>Signal Noise Ratio</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TR</td>
<td>Time Reversal</td>
</tr>
<tr>
<td>UWSNs</td>
<td>Underwater Wireless Sensor Networks</td>
</tr>
<tr>
<td>WAN</td>
<td>Wireless Area Network</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Wireless Fidelity</td>
</tr>
<tr>
<td>WBAN</td>
<td>Wireless Body Area Network</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WMAN</td>
<td>Wireless Metropolitan Network</td>
</tr>
<tr>
<td>WPAN</td>
<td>Wireless Personal Area Network</td>
</tr>
<tr>
<td>WSN</td>
<td>Wireless Sensor Network</td>
</tr>
<tr>
<td>WMSN</td>
<td>Wireless Multimedia Sensor Network</td>
</tr>
<tr>
<td>ZRP</td>
<td>Zone Routing Protocol</td>
</tr>
</tbody>
</table>
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thesis Title</td>
<td>i</td>
</tr>
<tr>
<td>Declaration by Student</td>
<td>ii</td>
</tr>
<tr>
<td>Certificate by Supervisor</td>
<td>iii</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>iv</td>
</tr>
<tr>
<td>List of Figures</td>
<td>vi</td>
</tr>
<tr>
<td>List of Tables</td>
<td>ix</td>
</tr>
<tr>
<td>List of Publications</td>
<td>x</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>x</td>
</tr>
<tr>
<td>Abstract</td>
<td>xvi</td>
</tr>
<tr>
<td>Chapter 1: Introduction</td>
<td>1-11</td>
</tr>
<tr>
<td>1.1 Wireless Networks</td>
<td>1</td>
</tr>
<tr>
<td>1.2 Sensor Networks</td>
<td>1-5</td>
</tr>
<tr>
<td>1.2.1 MANET</td>
<td>1</td>
</tr>
<tr>
<td>1.2.2 WSN</td>
<td>2</td>
</tr>
<tr>
<td>1.2.3 WMSN</td>
<td>2</td>
</tr>
<tr>
<td>1.2.4 IoT</td>
<td>3</td>
</tr>
<tr>
<td>1.2.5 IoMT</td>
<td>5</td>
</tr>
<tr>
<td>1.3 Applications of IoT</td>
<td>5-7</td>
</tr>
<tr>
<td>1.4 Ant Colony Optimization</td>
<td>7-8</td>
</tr>
<tr>
<td>1.5 Simulator Support for IoT</td>
<td>8-10</td>
</tr>
<tr>
<td>1.6 Thesis Overview</td>
<td>10-11</td>
</tr>
<tr>
<td>Chapter 2: IoT Protocol Stack and Architecture</td>
<td>12-19</td>
</tr>
<tr>
<td>2.1 IoT Architecture</td>
<td>12-13</td>
</tr>
<tr>
<td>2.2 IoT-A and ARM</td>
<td>14</td>
</tr>
<tr>
<td>2.3 IoT Protocol Stack</td>
<td>14-19</td>
</tr>
<tr>
<td>Chapter 3: Literature Review</td>
<td>20-41</td>
</tr>
<tr>
<td>3.1 Review based on Routing issue in IoT Networks</td>
<td>22-22</td>
</tr>
<tr>
<td>3.2 Review based on ACO supported algorithms for WSNs and MANETs for IoT Networks</td>
<td>23-25</td>
</tr>
<tr>
<td>3.3 Review based on Communication Technology heterogeneity in IoT Networks</td>
<td>25-27</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>3.4</td>
<td>Review based on Data heterogeneity in IoT Networks</td>
</tr>
<tr>
<td>3.5</td>
<td>Research Challenges</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Routing Issues</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Heterogeneity Issues</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Noise Issues</td>
</tr>
<tr>
<td>3.6</td>
<td>Research Approach</td>
</tr>
<tr>
<td>3.7</td>
<td>Research Objectives</td>
</tr>
<tr>
<td>3.8</td>
<td>Proposed Work</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter 4: Swarm Intelligence Routing Algorithm</strong></td>
</tr>
<tr>
<td></td>
<td>based on Communication Technology Heterogeneity</td>
</tr>
<tr>
<td>4.1</td>
<td>Different Technologies</td>
</tr>
<tr>
<td>4.2</td>
<td>ARAH-IoT</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter 5: Swarm Intelligence based routing algorithm</strong></td>
</tr>
<tr>
<td></td>
<td>to deal with data heterogeneity</td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>5.2</td>
<td>CARA-IoT</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter 6: Simulator</strong></td>
</tr>
<tr>
<td>6.1</td>
<td>Introduction to IoTRSim</td>
</tr>
<tr>
<td>6.2</td>
<td>How FANT and BANT works for the ARAH-IoT and CARA-IoT</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter 7: Results and Analysis</strong></td>
</tr>
<tr>
<td>7.1</td>
<td>Simulation Environment</td>
</tr>
<tr>
<td>7.2</td>
<td>Results based on ARAH-IoT</td>
</tr>
<tr>
<td>7.3</td>
<td>Results based on CARA-IoT</td>
</tr>
<tr>
<td>7.4</td>
<td>Results based on different simulations</td>
</tr>
<tr>
<td></td>
<td><strong>Chapter 8: Conclusion and Future Work</strong></td>
</tr>
<tr>
<td></td>
<td>References</td>
</tr>
<tr>
<td></td>
<td><strong>References</strong></td>
</tr>
</tbody>
</table>
ABSTRACT

Networks consist of a set of computers communicating data, where wireless networks send and receive data in a wireless manner. The nodes in the sensor networks communicate the data which is sensed from the surroundings. This data is primarily of scalar nature such as humidity, temperature, etc. and communicated in Wireless Sensor Networks (WSNs). The other types of data can also be communicated such as audio, video, image, text, or multimedia. These are Wireless Sensor Multimedia Networks (WMSNs) which send and receive multimedia contents. The vehicles or moving devices can also form the network known as Mobile Ad-hoc Networks (MANETs) which are self-configurable and without any centralized control.

Due to the advancement in technology, we are heading towards Internet of Things Networks (IoT), in which the smart objects and things can communicate using unique ID without human intervention. There is only device to device communication. The data is sensed and communicated among the smart devices. Here, also the IoT networks which are able to communicate multimedia content are known as Internet of Multimedia Things Networks. The Internet of Things networks may be formed using WSNs and MANETs. The things participating in the IoT ecosystem may be stationary or dynamic. The parameters related to the content or payload pose threat to the growth of IoT networks, those factors such as packet delay, noisy channel, latency, end-to-end delay, etc. are important and should be considered while investigating the path for the payload delivery from the source to the destination. The routing process in IoT networks is really a very big challenge and the researchers are working in this domain.

Also, the heterogeneity nature of IoT networks is posing a big issue when considering the growth of these networks. The heterogeneity exists at every level, horizontally and vertically in the IoT architecture. The protocol stack of IoT has various layers, where the heterogeneity is across the layers and within the layers among the devices.

This dissertation proposes a new routing protocol stack that considers the heterogeneity issues of IoT networks. This study mentions various kinds of heterogeneity that exist. The Data heterogeneity is considered while performing the routing protocol stack. According to the literature survey, the data heterogeneity...
which considers the different types of data such as audio, video etc. and the communication technology heterogeneity such as Bluetooth, Wi-Fi, Zigbee etc. These are identified as the most important challenges limiting the growth of IoT ecosystem. In this research, the algorithms have been proposed and designed for dealing with the data heterogeneity and also dealing the communication technology heterogeneity. The routing process becomes all the more difficult when the data has to be sent through noisy channel. The existing literature supports the use of middlewares or gateways while dealing with these issues but there are several problems associated with these architectures such as hardware support, failure rate and unreliability etc. Considering the gaps in the present literature, the new algorithms have been designed and implemented which are capable to find the best, reliable path and also takes into consideration various routing and heterogeneity metrics. The different types of data are sent through the noisy channel considering the SNR and BER. For handling the optimized path, the Ant Colony Optimization (ACO) approach based on swarm intelligence principle is applied. ACO is mostly used for finding the solutions for the optimization problems. According to the literature survey, it is found to be the best method which can be applied on the algorithms to find the optimized path in WSN. The dissertation also mentions the various simulators available and the problems associated with the same. Due to the mentioned problems, there is a need to design a new simulator. The simulator is designed in C# (.Net Environment) and the proposed algorithms are implemented. The proposed algorithms are compared with the standard protocols. The results clearly show that the proposed algorithms are supporting the IoT architecture and are capable of resolving the routing and heterogeneity issues of these networks.
Chapter 1

Introduction

1.1 Wireless Networks

As the technology is growing at a very fast pace, the communication has become possible without wires. Wireless networks are the type of computer networks which are cables free or wires free. The communication is possible through Radio waves. On the basis of range, there are various wireless networks exist such as Wireless Local Area Network (WLAN), where connection is possible through access points, Wireless Metropolitan Area Network (WMAN), connecting various cities and towns, Wireless Personal Area Network (WPAN), connecting person’s nearby devices and Wireless Body Area Network (WBAN), connecting various devices which a person is wearing. These networks offer less cost and high efficiency as these are cable less.

There are many other types of wireless networks that prevail in various forms such as:

1.2 Sensor Networks

The other type of networks which are used to generate and monitor the surrounding areas are Wireless Sensor Networks (WSN). The nodes are responsible to collect and send the data to the sink in these networks. These are low battery powered and resource constrained nodes capable of sensing scalar data such as humidity, temperature etc. The networks may have all moving nodes or mobile nodes, changing position frequently, forming the networks known as MANETs (Mobile Ad-hoc Networks).

1.2.1 MANET

The Mobile Ad hoc Network forms a temporary network with a collection of wireless moving devices without the centralized control and/or support services. In
these types of networks, the devices create the dynamic topology environment wherein these devices can enter and exit frequently. There is no fixed infrastructure for the configuration or the reconfiguration of the network [1]. The MANETs are mostly used in the meetings, military communications, disaster recovery situations etc. The participating nodes or the devices face the challenge of limited communication range. Every device moves on independently frequently changing its links to other devices. Each device acts as the router to forward the traffic from the source to the sink.

The multicast routing protocols are required. The various challenges faced in such networks are frequently changing topology, low bandwidth issues, less battery life etc. The protocols which offer the advantages such as high throughput, better power utilization, adaptable to dynamic topology, lesser number of payloads delays etc. are mainly required and much in demand. These factors if fulfilled may provide the Quality of Service (QoS) [2].

1.2.2 WSN

Wireless Sensor Network is the collection of various spatially distributed autonomous nodes forming wireless network topology, basically using the sensors and actuators to predict the surrounding environment. Most of the nodes in a WSN are stationary as compared to MANETs. Also, MANET offers the distributed computing whereas WSN is for the information gathering purposes. WSNs offer centralized control with low data rate. But both are distributed wireless networks involving multi hop routing, low battery nodes and which is self-organizing in nature [3].

1.2.3 Wireless Multimedia Sensor Network (WMSN)

There is also need to retrieve the different kinds of data such as audio, video, multimedia apart from only scalar data. WMSNs are the networks which are capable of sending and receiving multimedia content. These networks do not only improve the existing sensor networks but also extend the functionality of existing sensor networks. The presently available standard algorithms will not be able to suffice the needs of WMSNs, and the QoS-based, efficient and reliable algorithms are required.
1.2.4 IoT

The IoT networks are the networks of smart devices having unique ID for the communication. These smart objects send the data to and from, from the source to sink and maintains ubiquity and pervasiveness. These networks have sub networks as MANETs, WSNs, WPANs and WBANs, having no human to computer interaction and no human to human interaction. According to the Cisco survey [4], by the year 2020, we will be having 50 billion things connected world-wide. The researchers are working in this domain and several research challenges need to be resolved for such technology explosion.

There will be a huge ‘network of networks’ of uniquely addressable interconnected objects supported by standard protocols. The main aim of the IoT is to increase the persuasiveness and the ubiquity of the current internet and thus there would be integration of anything, anytime, anywhere and by anybody [5]. The things would be having embedded intelligence providing the distributed communication. Regarding the benefits provided by IoT, can be visualized as the device and device communication with less or no human intervention, more compatible surrounding environment for the living beings and also improving the quality of life. Currently, we are in the first phase of IoT development. There are several issues which are limiting its growth [6]. Lots of research has been continuing in the concerned area to provide the best of connectivity and efficient usage of resources of the network and the external networks. Several protocols have been designed and developed for optimum path selection. The path selection has been done on the basis of residual energy of nodes, number of forwarding nodes in the path, the occurrence delay metric etc. As the internet is growing at a much faster rate, the continuously increasing number of interconnected devices causes scalability problems. There will be the need of flexible infrastructure to deal with the various issues arising in the dynamic environment. Due to the heterogeneity of various standards and communication stacks, traditional measures cannot be followed or applied. The requirements of the IoT routing and communication protocols are similar to as that of the routing protocols for the MANETs (Mobile Ad hoc Networks) and the WSNs.
IoT can be considered as the extension of integration of both the MANETs and the WSNs.

![IoT technology stack](image)

**Figure 1.1 IoT technology stack [7]**

The Figure 1.1 provides the overview of the building blocks of IoT devices and system. It provides the insight into IoT technology stack. It lists the variety of connecting technologies ranging from short distance such as Bluetooth, ZigBee etc. to long distance such as 3G etc.

The Internet Protocol version 6 (IPv6) will be used to uniquely identify the objects in IoT networks and for routing traffic across the Internet. The current Internet Protocol version 4 (IPv4) uses 32-bit addresses and soon be limited for the unlimited number of devices in IoT. The IPv6 uses 128-bit addresses to provide the address to every device in IoT using IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN). 6LoWPAN establishes a low power wireless mesh network in which every node has the unique IPv6 address, connecting internet using open standards [8]. The increase in the number of connected devices per consumer will definitely lead to increase in Application Programming Interface (API) popularity also [9]. Several questions need to be answered:
• How to select the optimum path for data forwarding in multi-hop mesh networks?
• How to use the resources in the efficient manner?
• How to improve the reliability and scalability to the network?
• How to deal with the payload delivery issues in the network with respect to heterogeneity of the networks?
• How to increase the lifetime of the network?

1.2.5 Internet of Multimedia Things (IoMT)

For the pervasive and ubiquitous communication in the IoT networks, the communication for the multimedia content is also required. In IoMT networks, the various smart heterogeneous nodes can interact with each other using multimedia data. These networks have various stages like multimedia sensing, reporting and addressability, multimedia aware cloud and multi agent systems. These networks are the subset of IoT networks. The architecture is not same as that of IoT networks. As the IoMT networks contain WMSNs, the QoS is highly required to be maintained.

1.3 Applications of IoT

The various applications (Figure 1.2) of IoT are defined as follows [10,11]:

1.3.1 Smart Transportation

IoT smart devices which are enabled with sensors are very useful in case of Transportation domain. It includes various vehicle related monitoring or controlled driving techniques. IoT communications between the various vehicles has been proved very useful in safe driving and collision avoidance.

1.3.2 Smart Healthcare

Smart Healthcare includes monitoring patients’ health records and maintaining patients’ health. Specially, when the patient is at remote location, the IoT networks have been very useful. Even the doctors are able to give medical treatment using these sensors based IoT devices.
1.3.3 Smart Cities

Smart cities are coming up with the idea of making people’s life comfortable and easy. The devices are capable of handling the several issues like traffic light monitoring and controlling, collision detection, smart waste management etc.

1.3.4 Smart Agriculture

In agriculture domain also, the IoT devices are very useful. The agriculture machinery is sensor based and smart enough to take the decision such as when to spray the fertilizer, fertility of soil, smart irrigation etc.

1.3.5 Home Automation

Home Automation is the domain where all the devices within the building or home are connected and can communicate with each other. Based on the data sensed through the surroundings, the smart devices can behave and take decisions such as lighting control, temperature control etc.

1.3.6 Environment Monitoring

The IoT devices are able to sense the environmental conditions and behave intelligently in the emergency situations such as forest fire, floods, droughts etc. Based on the data sensed and analyzed, these can proactively warn for the worst situations.

Fig 1.2 Application areas of IoT [10]
The applications of IoT are not restricted to the above mentioned. The application area is very vast. The goal of IoT is to connect anything, anywhere, anytime and by anyone.

1.4 Ant Colony Optimization (ACO)

According to the literature survey, the swarm intelligence principle has been found very useful in solving the problems. Ant colony optimization is swarm intelligence-based approach to solve particularly the optimization problems [12, 13]. The first algorithm based on this approach was proposed in the year 1991. Since then it has been used with minor revisions according to the problem to be solved. ACO is metaheuristic-based algorithm which works according to probabilistic distribution.

\[
\rho_{ij}^k(t) = \frac{[\tau_{ij}(t)]^\alpha [\eta_{ij}]^\beta}{\sum_{k \text{ allowed}}[\tau_{ij}(t)]^\alpha [\eta_{ij}]^\beta}
\]  
Eq. (1.1)

Equation 1.1 \( \rho_{ij}^k \) is the Probability of ant k for choosing intermediate node i to reach source to node j (destination), \( \tau_{ij} \) is the amount of pheromone from node i to node j. \( \alpha \) and \( \beta \) are the two values for calculating the probability of best solution i.e. best route. Their values range between 0 and 1. Both these are used as heuristics like the importance given to distance during calculating the path values and importance given to pheromone deposit on the path. Generally taken as:

Values for \( \alpha = 0.7 \) and \( \beta = 0.7 \)

\[
\tau_{ij}(t + 1) = (1 - \rho)\tau_{ij}(t) + \Delta \tau_{ij}(t)
\]  
Eq. (1.2)

In Equation 1.2 (for BANT), the evaporation of the pheromone is taken into consideration. It says that at time (t+1), the probability is subtracted from 1, multiplied with the pheromone value and added to the change in the value of pheromone of previous time is considered.

\[
\Delta \tau_{ij}^k = \begin{cases} 
\frac{1}{L_{kj}} & \text{if } (i, j) \in \text{path} \\
0 & \text{Otherwise}
\end{cases}
\]  
Eq. (1.3)
Where \( L_k \) is the constant taken into consideration if ant \( k \) chooses node \( i \) to travel to node \( j \). It basically tells the value by which the pheromone value should be increased.

In the ACO based approach, various parameters are taken for the calculation of pheromone such as delay, hop count, distance etc. The algorithms proposed in this dissertation uses other metrics for the calculation of pheromone, to find the shortest reliable path such as packet loss, speed, no. of conversions etc.

**1.5 Simulator Support for IoT**

Simulators have always been used for imitating the real scenarios which otherwise are difficult to test. These are basically combination of hardware and software, which provide the modelling feature of the real case. Simulators consider all the factors which are crucial for the development of the solution and the problem under analysis.

There are various simulators available for the development of the IoT solutions. All these have their own features, limitations and suitability to various layers of IoT architecture. Some of the simulators [14] are briefly explained as under:

**1.5.1 OMNet++**

The OMNet++ is one of the most popular network simulators available freely on the internet. This is particularly used for the WSN research. Although the support for the mobile adhoc networks is also available. This simulator offers wide variety of features. The paper [14] clearly states that this simulator lacks the support for IoT models and also does not offer much for the application layer protocols.

However, the ACO support is there but inclusion of new parameters and models is still required and to be done manually.

**1.5.2 NS3**

The NS3 simulator, is specifically used for the WSN network simulations and is the successor of the NS2 network simulator. This is the most widely used simulator for IoT networks. But like OMNet++, it also lacks support for application layer
protocols for IoT. It has ACO support but full support for network parameters is not seen such as heterogeneity metric and different communication technologies.

1.5.3 CupCarbon

It is the simulator for IoT which works for the mobile nodes in the real-world environment. The nodes are placed and simulation is carried to check for the mobility of nodes in IoT environment. It is suitable for the network layer mobile nodes but does not support application layer protocols. Incidentally, at present, there is no ACO support. The node parameters are limited and simple.

1.5.4 Cooja

Cooja is the simulator which is available for IoT simulation. It is one of the popular simulators which is used specifically for the Contiki operating system. The IoT sensors can be placed and tested but has some limitations as well. First, support for ACO is not there and also the sensor nodes are deployed matching the physical hardware in simulation. Therefore, it basically acts as the emulator instead of a simulator, which is not much suitable for IoT network simulations.

1.5.5 Qualnet

The discussed simulators are freely available but there are other simulators also which are not freely available. The Qualnet simulator is one of the commercial software. It also supports the heterogeneity concept of the IoT networks and also has the Sensors Network Library for carrying out the IoT simulations. It also supports ZigBee devices. But as it not open source, its use is limited and it becomes difficult to use the simulator software. Other such commercial simulators are also available but this can be analyzed that due to wide variety of available simulators, it becomes difficult and challenging to choose from these. The paper [14] clearly mentions that there is no all-in-one simulator available for IoT networks. The detailed comparison of the simulators is available in the Table 1.1.

Table 1.1 Current IoT Simulators’ features where No-not supported and Yes-supported
<table>
<thead>
<tr>
<th>Simulator</th>
<th>Language Supported</th>
<th>ACO Support</th>
<th>Mobility Support</th>
<th>Communication Tech. Heterogeneity</th>
<th>Open-source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cup Carbon</td>
<td>Java</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>OMNet++</td>
<td>C++</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>QualNet</td>
<td>C/C++</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>NS3</td>
<td>C++</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cooja</td>
<td>C/Java</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

After working on all the simulators mentioned in the table, it has been analyzed that there is no simulator available for IoT architecture which is suitable for all the layers, which is open-source, which supports heterogeneity and other crucial parameters and also which supports ACO approach. No such combination exists for the development of IoT ecosystem.

A new simulator is designed in C# (.Net environment) – IoTRSim (IoT Routing Simulator) for dealing with the routing and the heterogeneity issues of IoT. The various parameters have been taken for the nodes for the simulation.

### 1.6 Thesis Overview

The thesis examines the issues, challenges and opportunities of IoT. The existing heterogeneity challenges are reviewed carefully by considering all the facts and figures. The two heterogeneity issues such as communication technology heterogeneity and the data heterogeneity are reviewed and analyzed carefully. The impact of these two heterogeneities are taken into full account to design our proposed algorithms. The dissertation has eight chapters that explain the flow of work with proper simulator implementations and results analysis.

- Chapter 1 provides the introduction to Wireless networks and IoT networks. The applications of IoT are mentioned and the various types of simulators available for IoT are also discussed.
• Chapter 2 mentions the IoT architecture, protocols and protocol stack in detail. It describes the architectures which can be used in the communication of the IoT devices.

• Chapter 3 investigates the literature survey of IoT network issues such as routing and heterogeneity etc. It also mentions the various research challenges, the research objectives and the proposed work.

• Chapter 4 explains the communication technology heterogeneity w.r.t IoT in detail. The swarm intelligence routing algorithm has been proposed in this chapter to resolve the communication technology heterogeneity of the IoT networks – ARAH-IoT.

• Chapter 5 explains the data heterogeneity in detail and a swarm intelligence algorithm has been proposed to deal with the data heterogeneity in the IoT networks- CARA-IoT.

• Chapter 6 introduces the simulator designed and developed in C# (.Net Platform). The algorithms ARAH-IoT and CARA-IoT have been implemented on the simulator.

• Chapter 7 Results Analysis has been done in this chapter. The results are mentioned on the basis of communication technology heterogeneity (no. of conversions) and on the basis of data heterogeneity (SNR) in IoT networks.

• Chapter 8 summarizes the dissertation. The conclusion is drawn and also the future work is mentioned which can be done by the researchers. The last section is dedicated to the references used in the thesis.
Chapter 2

IoT Protocol Stack and Architecture

2.1 IoT Architecture

IoT is the upcoming domain to connect the devices enormously. The IoT architecture is planned as such to merge various technologies [15]. The entities participating in IoT network may be sensors, actuators, protocols, intelligent devices etc.

![IoT Communication Infrastructure][1]

The Figure 2.1 shows the communication infrastructure of IoT ecosystem. At the lowest layer, there are sensors and actuators, which collect information from the surroundings. There is connectivity among the smart devices at this layer. Above it, the layer is composed of Gateways and Network communication devices. The data collected in the previous layer by the sensors is passed through the middle-
wares or gateways. The next is the Management and the security services layer, which actually analyze the data passed from the gateways and inferences are made. Above all the layers is the Applications layer, which has all the smart applications used by the users for the comfort and ease.

For the delivery of quality products [16], there is need for the standard IoT architecture. A planned and comprehensive architecture is required to suffice the present and the future needs of the IoT market.

The first block in the Figure 2.2 mentions the 3-layer architecture, the perception layer, the network layer and the application layer. The second block represents the 5-layer architecture including the middleware layer. Middleware layer is acting the interface between the network and the application layers. The third block has the objects at the bottom most layer, the data is produced at this layer and passed on to the service management layer using the various communication technologies such as ZigBee, Wi-Fi, Bluetooth etc. at the object abstraction layer. And the last block states the layered model with Business layer at the top most level, responsible for managing all the IoT activities and services.

2.2 IoT-A and ARM

The European Commission [17] took the initiative to deal with the issue of common IoT architecture problem. The International IoT Forum was established to create
the common IoT architecture. The IoT-A project has been developed to focus on the planned and common architecture design. The primary objective of this project is to state the reference model known as Architectural Reference Model (ARM) to build the common IoT architecture. The main aim of the ARM is to mention the factors that can be used to build the architecture instead of stating the single architecture. So that the different architectures can be build based on the requirements of the different applications using the factors identified by the ARM.

2.3 IoT Protocol Stack

The IoT Protocol stack is the extension of the standard TCP/IP protocol [18]. The stack can be viewed as follows:

![IoT Protocol Stack](image)

**Fig 2.3 IoT Protocol Stack (a) [18]**

It consists of various layers with a number of protocols for the specific requirements. In the Figure 2.3, the TCP/IP mapping is done with the IoT protocol stack. And it can be seen that TCP/IP Application layer is divided into two layers namely Application Services and the Application Protocols. The various protocols which can be used at different layers [19] are presented as under:
The protocol stack of IoT contains several layers as seen in the Figure 2.4. At every layer there are various issues also associated. The layers mentioned in the stack are:

- Link Layer
- Internet Layer
- Transport Layer
- Application Protocols Layer
- Application Services Layer

The link layer has several challenges such as related to traffic, related to devices, related to access to devices or data and also the scalability. The IoT may include the fully resourceful nodes to the highly resource constrained nodes. The resources listed as constrained can be in terms of processing power, energy of the nodes etc. whenever the nodes need to communicate in the network, the energy of the nodes deplete faster, So the devices should be smart enough to deal with the constraints and also provide efficient communication in the network. The link layer includes the framing, retransmissions, device communication issues etc. The traffic in the network varies and depends on the application to be used. Some applications may be very tight regarding the QoS parameters whereas other applications may be very flexible regarding the same. Like scalar data may involve very less traffic but transmitting video packets may involve heavy traffic load in the network. The access in the IoT network may be through wires or wireless technologies. Also,
these technologies are expected to work for the long-range communication or the short-range communication and also considers mobile as well as stationary objects in the IoT networks. Also, the scalability is highly required for the wireless communication of the IoT network devices. The networks face several scalability issues.

Internet Layer - The IoT networks have vast number of smart devices which are resource constrained that is which offers very limited power, limited processing, limited memory etc. Usually called as Low Power Lossy Networks (LLNs), contains various smart devices connected through available long range and short-range communication technology. Presently, energy is taken up as the most important issue and several protocols have been proposed to reserve the same. But other factors should also be considered while designing the routing protocols for the IoT networks such as node speed and the device ability. The node failure should be taken into consideration as well as the link quality. To resolve the issue, 6LoWPAN has already been proposed and useful in fragment and reassembly of packets. It is basically responsible for the IPv6 packet header compression, IPv6 packet segmentation, reassembly and forwarding of the packets.

The Application protocol layer is responsible for the efficient communication between the applications, smart objects and the gateways or middleware. All the protocols involved in this layer are responsible for exchanging data between the devices. Presently, several application protocol layer protocols have been offered, each with the list of various strengths and weaknesses. The maintenance of QoS is highly required using application layer protocols.

There have always been very tight constraints while connecting the applications and the devices. The Application Services layer (Figure 2.5) act as the abstraction layer for the connectivity of various devices with the large number of applications. It acts as the middleman for the working of varied applications and the seamless connectivity. It provides the interoperability among the various applications and the devices.
The variety in the IoT protocol stack has led to the various issues regarding the protocols and these standards demand the uniformity in the IoT architecture. The solutions or the standardization are required. The IoT framework is required which covers all the layers of the protocol stack, covers the participating devices, the network and suitable for the developed tools and the standards.

Different architectures are available for the development of the IoT framework. From which the two architectures are more important i.e. 3 layered architecture and the 5 layered architecture.

The 3 layered architecture (Figure 2.6) is known to be the famous and basic IoT architecture. It mainly has 3 layers i.e. application layer, network layer and the perception layer. The bottom most layer is the perception layer which includes all the smart sensor-based devices which are able to collect the data from the environment. The collected data is further sent to the above layer i.e. Network layer. The network layer consists of all the wireless and the wired communication technologies and is responsible for providing connections between the devices and the applications of the IoT ecosystem. The sensed data is passed on to the application layer, where it is analyzed and the results are computed, and passed on back to the perception layer from the application layer through the network layer.
Fig 2.6 The 3-Layered IoT architecture [20]

The Figure 2.7 shows the five layered architecture, which mentions that it is the extension of the three-layered architecture and has two more layers namely gateway and the middleware. The basic layers of the 3 layered architecture will work as it is, but the gateway layer and the middleware layers provide the connection between the various devices and the applications.

There is a huge number of applications possible in IoT framework. But the constraint is that all the devices which are going to provide all these applications run on their respective systems or platforms. No uniformity is currently present. Big companies are busy in developing their own products, smart devices and applications. Standard protocols are not being followed. They have their own standards which makes the process of interoperability very difficult.
So, the standardization in case of IoT architecture is highly required as there is vast variety in IoT networks. As it is said, “The Internet of Things Might Never Speak a Common Language” in [20], the efforts need to be compulsorily made for the standardization and the interoperability.

If the standardization is implemented successfully, it will in turn automatically lead to interoperability among the various devices and platforms provided by the different vendors. And in turn, it will also provide the security for the devices participating in the IoT network.
Chapter 3

Literature Review

The IoT is developing in the stages. The initial stage of IoT needs several issues to be resolved. Various algorithms have been already proposed for the MANETs and the WSNs. These algorithms may follow reactive, proactive or hybrid approach. These currently proposed algorithms may behave like standard algorithms for the growth of IoT. More such efficient protocols are required to be developed especially for the IoT architecture [21]. The algorithms can be proposed based on the swarm intelligence principle so as to achieve the goal efficiently. This literature review explains existing swarm intelligence-based protocols and the solutions for the IoT development.

3.1 Review based on Routing issue in IoT Networks

The authors in [22] have proposed the algorithm which is for IoT networks and is based on the Adhoc on demand multipath vector distance protocol, which works on the principle of updating the internet connecting table and selects the stable transmission path. The routing overhead is increased in the transmission process but the average end-to-end delay is decreased.

The authors in [23] mention that mostly the sensor networks are implemented using gateways and these are based on number of protocols. The gateways are beneficial in various ways such as capability, security etc. The gateway approach which has been used in the paper is dynamic priority scheduling based. This proposed research offers several advantages like delay and data concurrency.

The authors in [24] mention that the IoT will have the smart devices as the primary user. Rather than the human to device communication there will be Device to Device communication without the centralized control. This D2D communication will requires the smart routing protocols to enable the intelligent communication. The paper also analysis the standard routing algorithms for the intelligent communication and also identifies the various challenges associated with it. The
authors discuss various categories of algorithms to deal with the routing issues of the IoT networks and also mention the future challenges.

The authors in this paper [25] have termed the IoT as next generation Internet. The paper proposes the routing algorithm which considers the congestion, the interference and the energy of the sensor nodes. The proposed algorithm particularly works for the remote health care monitoring applications. The algorithm considers the SNR of the hops, noise and also the congestion.

The authors in [26] state that the IoT is emerging as the upcoming technology. The smart things in the IoT network communicate using intelligent interfaces to connect with the user contexts and the social environments. The paper surveys the existing standard protocols such as OLSR, DSR and AODV which are the basis of routing in the Adhoc networks. The environment is setup for the things to behave in the IoT environment and various metrics are checked such as end-to-end delay, throughput etc. The results clearly showed that the DSR is better in terms of routing overhead whereas AODV is better in case of throughput.

The paper [27] mentions that the things in the IoT networks connect by making the things smart which involves sensing data, reasoning and co-operation between the things. The author mentions the various advantages of IoT and suggest that middleware is the foundation of the IoT architecture. The paper mentions various publish / subscribe algorithms.

The authors in the paper [28] mention about the Underwater Wireless Sensor Networks (UWSNs). These networks require increased life time and face various problems such as attenuation, limited bandwidth and limited processing power. The authors propose a new energy efficient routing algorithm i.e. Balanced Energy Adaptive Routing – BEAR to increase the lifetime of these underwater wireless sensor-based networks.

The authors in this paper [29] mention that the traditional approach followed for the neighbor discovery in the network was to check for the energy of the nodes but the introduction to the mobility of the nodes has posed problems to choose the neighbor and the process of neighbor discovery has become quite challenging. The opportunistic networking requires the short-range connectivity opportunities in the
IoT networks to deliver the payload. The concept of opportunistic networking can be applied to devise new routing algorithms to implement the knowledge driven networks.

The authors [30] mention that recently the IoT has gathered interest from the researchers and the academicians. They recommend that the mesh topology of the IoT networks will be successfully using the multi-hop routing. They investigate the trusted connectivity probability to allow the device to device communication in the multi-hop routing in IoT networks. The 5G scenario has been considered in the paper and also the shortest route is found, keeping the base stations fixed or random, as per the requirement. The routing algorithm has been proposed to achieve the highest trusted connectivity probability.

The paper [31] mentions that sensor-based data is captured and forwarded by the machines in the network using M2M gateways. The authors suggest that new routing algorithms are required as the present algorithms have the disadvantage of non-uniform consumption of energy by the sensor nodes and also the extensive use of the limited resources of the sensor nodes. The paper proposed a hybrid routing protocol to overcome these issues for IoT wireless applications. The results clearly show the reduced energy consumption and improved network lifetime.

The authors [32] have suggested and proposed a protocol LOADng to remove the drawbacks of AODV and RPL protocols. The proposed algorithm is proved better in terms of reduction in the number of packet loss, latency and consumption of energy.

The paper [33] mentions that in IoT applications, there is a concept of self-organization and connectivity between various smart objects. In the present scenario, mostly the topology which is followed is point to point. The author presents the MANETs and also explain the various challenges associated with these networks such as limited power supply, short range communication, intermediate node failures etc. A protocol - CRRP is mentioned which consumes less energy and reduces the interference.
3.2 Review based on ACO supported algorithms for WSNs and MANETs for IoT Networks

The authors in [34] propose the ACO algorithm which is based on self-organization and dynamic routing. This algorithm is proposed for the WSNs and works in three stages, firstly neighbor discovery, secondly, the routing and packet transmission and lastly, the route maintenance. In the first phase, the routing tables are created based on the request, secondly the shortest path is chosen for the delivery of the payload and in the last phase, the routing tables are updated based on the routing information and ACO also discards the node which are of low energy. The paper compares the ACO with the other algorithms, the node operational time and average energy consumption is compared. The comparison shows the efficiency of ACO algorithm, and how effectively the swarm intelligence is used and applied for the denser networks.

The authors in [35] proposed the algorithm, for the Mobile Ad-hoc Networks. The algorithm AntHocNet follows the hybrid approach and finds the shortest distance on the basis of ACO. The forward ants are responsible for the path setup phase and the backward ants are moved from the destination to the source. The tables are created to calculate the path quality using pheromones. The path quality is measured using the pheromone received by the backward path, for the path chosen by the forward ant. The AntHocNet proactively finds the working nodes and updates the routing table if there is any link failure(s). Authors have compared the AntHocNet algorithm with the standard AODV (Adhoc on demand Distance Vector) protocol and finds that the AntHocNet is proved to be better in terms of delay, jitter and delivery ratio.

This algorithm was proposed in [36] to improve the performance of multipath routing. The protocol is based on the AODV routing protocol also adds the ACO functionality to AODV. The best neighbor node is selected on the basis of average load of the route, hop count and the average link count of the route. The quality of service is maintained by regularly updating the routing tables and selecting the next
The ACO-AOMDV is compared with the ARA and the AOMDV protocols. The proposed protocol in this paper has been proved better than the protocols in comparison in terms of packet delivery, average end-to-end delay and other such routing metrics.

The paper [37] proposed the algorithm PERA which is swarm intelligence-based protocol and beneficial for the wireless networks. The algorithm works on the feedback mechanism. The ants are used for route discovery and for calculating the best path. The forward ant finds the route to be followed and the backward ant maintains the routing tables by frequently updating the path quality in terms of path goodness. The feedback factor by the backward ant is not mentioned in the standard algorithms such as AODV and DSR etc. The packets are communicated using the routing path provided by the backward ant. The comparison is made with the AODV in this paper. The algorithm PERA is useful in increasing the throughput, lowering the average end-to-end delay etc.

The authors in [38] mention the routing protocol which is reactive in nature and proposed for the WSNs. The protocol has extended the standard algorithms HOPNET and ZRP. The proposed algorithm in this paper considers the dynamic topology dealing with congestion and failed links. AD-ZRP is based on the HOPNET which considers the zones and on the ZRP which is proactive in nature. The route discovery is interzonal and intrazonal. The zones are added on demand after the packet transmission is made. The route discovery is done on the basis of the pheromone. The protocol is compared with the HOPNET protocol and achieves greater efficiency in terms of congestion, packet delivery ratio etc.

The authors in [39] also proposed the algorithm, EEABR, for the WSNs. This algorithm considers the various WSN issues such as low power, low memory and low processing. The ants reach the destination travelling from the source using intermediate nodes and find out the shortest best path. EEABR calculates the routing path on the basis of energy efficiency of the path and the number of hops in the routing path. The authors have compared the EEABR algorithm, with the other
two algorithms Backward Ant-Based Routing (BABR) algorithm and Improved Ant-Based Routing (IABR) algorithm. The results in the paper show that the proposed EEABR algorithm, is efficient enough to save the energy and reduces the communication load.

The algorithm ARAMA is proposed in the paper [40]. The protocol is also swarm intelligence based and considers the dynamic changes of the network. The most important metric which is used in ARAMA for calculating the best reliable path is hop-count. Using this algorithm, the energy of the nodes is maintained in the network. The nodes are provided with the energy on the priority basis.

The author in the paper [41] mentions that there is need for the routing algorithm in IoT networks. The ACO approach has been followed to propose the routing algorithm for the IoT networks.

The authors in the paper [42] mention that the IoT is the connection between the physical as well as the digital entities. The paper considers the IoT development and agent-based computing is discussed. The benefits of using the swarm intelligence have also been mentioned. The ACO based model has been proposed for the IoT applications.

3.3 Review based on Communication Technology heterogeneity in IoT Networks

The authors in [43] mentions the pervasiveness of the IoT networks. They state that the current solutions are not suitable enough for the reliable connectivity of the smart things in the IoT networks. The IDRA architecture has also been evaluated in the paper. The gateway approach has been represented as the solution for the future generation networks. But the gateway approach has several disadvantages like packet overload, low battery, low throughput etc. The IDRA architecture proposes the solution for the direct connection between the wireless and wired devices having different communication technology. This architecture mentions that whenever the packet of a communication technology is converted into other technology, the packet takes 6.37 ms. This conversion time is significant in the routing process and should be considered.
The paper [44] tells that to successfully manage the IoT applications and services, its architecture must be well designed. The paper mentions the various issues in the current IoT ecosystem. It has been mentioned that the existence of various technologies in the IoT networks lead to communication problem, where the gateway approach is the only present solution. The greater number of solutions are required to deal with various issues of the IoT networks. The network layer is primarily focused here. A novel IoT network architecture has been proposed in the paper.

The authors in the paper [45] propose a multi interface gateway to deal with the device and technology heterogeneity in IoT networks. It takes into consideration the time conversion also between the different technology packets. The packet structure is also mentioned to deal with the heterogeneity in IoT networks.

The paper [46] mentions that due to the complexity and heterogeneity present in the IoT networks, the present routing algorithms are not sufficient enough for communication in the IoT networks. The paper proposes a new smart and energy efficient routing algorithm to maintain the quality of communication in IoT networks and also considers the new parameters of the various devices in the IoT networks.

The authors in [47] say that the heterogeneity in IoT is the most liked field by the researchers. They also mention that due to the heterogeneity of the architectures and as well as the heterogeneity of communication technologies, there are many challenges which need to be addressed to for the robust IoT networks. The paper proposes a new 4 layered architecture which is suitable enough to deal with the mentioned issues.

The authors in [48] mention that currently what we are using is the fixed internet and heading towards the mobile internet with the collection of smart objects such as smart phones, tablets etc. The focus of the paper is to mention the communication architecture to provide the connectivity in IoT. The paper discusses many of the layers of the stack and also list the shortcomings.
The authors [49] mention that IoT involves the communication of smart objects such as actuators, mobile phones, sensors etc. Various communication technologies are involved in the routing process of IoT networks. Authors state that IoT involves WSNs and WMSNs. Where every WMSN act as a gateway for the WSNs to transfer the data using short range communication technology such as ZigBee and Bluetooth.

The authors [50] mention that IoT is the interconnection of the cyber space and the physical world of the smart objectives. The trend of the networking has been changed and the revolution in IT has led to the new trends in future networking. The authors discuss the various traditional technologies related to IoT and present the challenges and problems with respect to the IoT development.

3.4 Review based on Data heterogeneity in IoT Networks

The authors in [51] focus on the energy efficiency in MANETs. There are several parameters which are required to be considered such as real time communication, bandwidth, packet broadcast overhead etc. Due to these issues, the standard routing protocols are required. Along with these, the SINR also plays significant role while selecting the communication path. The authors suggest that SINR should be taken into account. They mention that SNR and BER are the best metrics for finding the reliability of the link and also in case of every packet received the metric, Link Packet Error Rate (LPER) is used for maintaining the QoS in the network.

The authors in [52] have stated the emergence of WMSN networks from the WSNs, which deal with the multimedia data instead of the scalar data. The authors explain the three WMSN architecture, single tier, single tier clustered and multitier. The challenges in the WMSNs are explained and the importance of maintaining the QoS is identified. The standard algorithms which are presently available mainly consider the congestion and not noise.

The paper [53] investigates the use of Adhoc networks in real time applications. The real time data can also be communicated from the source to the destination. The multimedia content transferred has several challenges in the network. The
paper mentions the challenges while transmitting image data. The low energy of the nodes adds up the big challenge while communicating image data. The algorithm is proposed which deals with the issues of multimedia and the QoS parameters have been studied.

The authors in [54] discuss the WMSN networks in detail. The paper mentions the current WSNs scenario and the future work for the WMSNs. The survey of various available architectures, algorithms and protocols has been provided for the various layers of these networks. The authors suggest that swarm intelligent nodes are also better for the wireless sensor multimedia networks. They also state that standard algorithm TCP, cannot be used in WSN and WMSN as TCP mostly considers the congestion alone and also generates connection establishment overhead.

The paper [55] mention that the WSNs have large variety of multimedia applications. The requirements of these applications are to maximize the QoS and minimizing the energy requirements specifically for the video applications. The paper proposes the scheme for the efficient video communication which achieves both the requirements.

The authors in [56] mention that the WSMNs are useful in making real time applications but QoS poses several routing challenges. The paper presents the growth of various routing protocols for using multimedia content in the networks and also highlights the need of other multipath routing protocols for the WMSNs.

The authors in the paper [57] states the requirement of different communication standards due to the different bandwidth capabilities. The paper deals with the heterogeneity in bandwidths and the proposes the Time Reversal (TR) approach. It offers the energy efficiency of Terminal Devices and Access Points. The paper states that there are varying requirements for different types of device in the communication such as QoS, hardware capability, bandwidth etc. The middleware approach has been proposed in this paper.

The author in the paper [58] has proposed a framework to deliver the data in disaster management networks. The data from the sensor node is transferred to the large-scale network using the gateway such as Internet. The author mentions that the
static topology has not been followed in case of IoT networks as in WSNs. The random topology poses several challenges with respect to the routing issue in the IoT networks. The author suggested that for the best routing operation in disaster inspired networks, the cognitive energy-efficient approach is to be applied.

The authors in the paper [59] suggest the need of the routing protocols for the MANETs. The authors mention that several routing protocols exist but more efficient protocols are required to maintain the QoS in the MANETs. As these networks are highly dynamic in nature, routing in the multi-hop scenario becomes very challenging. The position-based routing protocols and topology-based protocols are discussed and evaluated. And also need of more such position-based routing protocols is highlighted.

The paper [60] takes into consideration the development of the sensor and vehicular network which is of hybrid nature mainly for the transportation system. The emergency situations are surveyed and a framework has been proposed that enable the communication of the multimedia data in the smart cities’ networks. A mathematical model has also been proposed to route the data packets efficiently and maintains the quality of service.

The paper [61] mentions the importance of geographic routing in MANETs. The authors propose a routing algorithm which is a position based and also takes into consideration the QoS. The quality nodes are chosen on the basis of SNR.

The authors in the paper [62] mention that the routing plays a vital role while communicating the payload in the IoT networks using the sensor nodes. The paper provides the literature review based on the QoS, network lifetime, energy, node deployment etc. The routing protocols are also compared on the basis of latency, average end-end delay etc.

The authors in the paper [63] mention the need of the IoT architecture. The authors propose a data driven architecture for the IoT ecosystem. The data cycle is studied to know the transformation process of data. A new framework has been proposed to deal with the IoT data services. The beauty of the new framework DataTweet is
to provide the ubiquitous data service to enable the transmission of short data messages to the computing platforms.

The authors [64] present the IoMT as a new field which is attracting the researchers. Presently the scalar data is being given much importance instead of exploiting the multimedia capability of the IoMT networks. The paper proposes a cross layered protocol for the multimedia networks. The paper clearly states that due to the hardware heterogeneity in the IoT networks, the presently available routing algorithms are not suitable for the communication in the IoT networks.

### 3.5 Research Challenges

IoT can be defined by the means of various challenges which further can be categorized by a word i.e. scale. As we know that the various MANETs and WSNs collectively lay the foundation for the IoT architecture. A MANET or a WSN can be part of an IoT but not vice versa. Every challenge that is known for the MANETs or WSNs in the current scenario also exist for IoT implementation and again with respect to it scale or granularity, the implication is even harder.

Routing is the major challenge for the payload delivery from the source to the destination in the network. Several significant factors are missing in case of all the existing protocols available for MANETs and WSNs [65]. The existing protocols do not solve all reliability issues and efficient routing is not achieved still completely. As of now, no techniques or protocols are efficient enough to cover all the issues and provide the solution. There is a need to develop new protocols for the communication which will cater all these needs [66]. The existing standards are not considering the effect of noise in the routing and payload delivery process fully. Any heuristic approach has not been found for content delivery in IoT, based on Signal Noise Ratio (SNR) [67].

As internet is transforming into IoT, it introduces the level of complexity with respect to interoperability (such as vendor interoperability) [68,69] or heterogeneity of things like RFID (Radio Frequency Identifiers), sensors and other devices. The standard protocols are lacking in handling the same. Two important issues need to
be considered, firstly, implementation of IPv6 over 6LOWPAN (to connect every small device in IoT) and secondly, standardized protocols for the machine to machine communication.

Efficient and scalable routing protocols adaptable to different scenarios and network size variation capable to find optimal routes are required. The usage of ACO principles in the routing algorithms, prove to be bright for the route optimization issues.

The rise of IoT networks poses more and more challenges for the sensor networks and several opportunities [70]. The IoT generates that amount of data which is even difficult for clouds, the traditional systems and the edge computing to manage. The routing issues include the metrics such as packet delay, quality of the routing path, lifetime of the nodes, jitter, node failure, throughput etc. There is the need for reliable payload transmission from the source to the destination for scalar as well as multimedia content [71].

The steps of processing data from collection to distribution of context with respect to sensor data play a very important role [72]. The IoT is proving to be a global platform for establishing the communication between unlimited numbers of devices. But the connectivity between these smart objects poses to be great challenge [73]. The need is to develop new technologies and solutions to enable IOT in practice. Efficient, reliable and inter operations are required for Device-to-Device (D2D) communication for the IoT ecosystem [7,74].

3.5.1 Routing issues

The data cannot be sent directly from the source to the sink. The multi hop mesh topology requirement lays emphasis on the fact that it has to travel through an efficient route involving sensor nodes [75] to reach the desired destination. The routing process can be categorized in the following ways:

- Routing based on the network structure - It includes the flat based routing in which every node participates in the network and plays the same prescribed role. In horizontal routing, only high energy nodes are selected for the route
formation. And in the Location based routing, the sensor nodes are identified using signal strength parameter and are controlled through Global Positioning System (GPS).

- Routing based on the protocol operation- In Multipath selection routing, the route is chosen among the various available paths, compromising on energy resource. In query-based routing, the communication between the sender and the receiver is through queries. In Negotiation based routing, the negotiation is done to eliminate the high level of data redundancy.

- Routing based on how the source finds out the destination- The Proactive type of protocols; the route is decided before the need arises. Whereas the Reactive type of protocols, decide the route only when such demand arises in the network. In the Hybrid type of protocols, these offer the mix of proactive and reactive protocol categories.

- Routing based on the communication initiator- The request to send or receive the data may arise from the source or the sink, deciding on the initiator of communication category.

- Routing based on the criteria of selecting the neighboring node- In the Content based routing, the content or the kind of the data is more focused upon for the route selection. In the Probabilistic routing type of protocols, there is random selection of the neighboring nodes for data transmission. In the Broadcast routing methods, each node re-broadcasts the message and if undelivered, it is dropped.

The successful transmission of data requires the reliable communication between the smart things in the Internet of Things network. And for the communication process, the various technologies can be used ranging from short range ZigBee to long term GSM. As IoT is considered the combination of different MANETs and WSNs, several factors need to be highlighted, which are mentioned as follows:

Table 3.1 Factors affecting MANET, WSN and IoT
<table>
<thead>
<tr>
<th>Parameter</th>
<th>MANET</th>
<th>WSN</th>
<th>IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multipath</td>
<td>Considered</td>
<td>May not be Considered</td>
<td>May not be Considered</td>
</tr>
<tr>
<td>Dynamic Technology</td>
<td>Considered</td>
<td>May not be Considered</td>
<td>May not be Considered</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>Considered</td>
<td>Considered</td>
<td>May not be Considered</td>
</tr>
<tr>
<td>Network Lifetime</td>
<td>Considered</td>
<td>Considered</td>
<td>May not be Considered</td>
</tr>
<tr>
<td>Improvement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-hop Routing</td>
<td>Considered</td>
<td>Considered</td>
<td>May not be Considered</td>
</tr>
<tr>
<td>Link Failure</td>
<td>Considered</td>
<td>Considered</td>
<td>Considered</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link Quality</td>
<td>Considered</td>
<td>Considered</td>
<td>May not be Considered</td>
</tr>
<tr>
<td>Energy Efficiency</td>
<td>Considered</td>
<td>Considered</td>
<td>Considered</td>
</tr>
<tr>
<td>Heterogeneity</td>
<td>May not be Considered</td>
<td>May not be Considered</td>
<td>Considered recently</td>
</tr>
</tbody>
</table>

The Table 3.1, mentions some of the factors which should be given due importance while designing new routing algorithms for IoT. The factors are considered in MANETs and WSNs but most of these are not currently considered in case of IoT. The table clearly show the current status of the growth of IoT ecosystem. The reliable, robust and comprehensive algorithms are required for the fast paced IoT development. Recently, much focus is given in the heterogeneity area in IoT, but still there are open issues which need to be resolved as soon as possible.

There is no standard algorithm exist presently, to work in the heterogeneity domain of IoT networks. Heterogeneity is very vast and is found at every layer in the IoT architecture. Also, the routing algorithms can be designed which include some more parameters which are listed as under.
- Context Awareness – Context of the node is the surrounding environment of the node such as location, the CARA of the sensor node etc. Most of the routing protocols in the above table are context aware [76]. This metric is useful while calculating the error free, failure free route with minimum delay and maximum packet delivery ratio and throughput. The SNR can also be considered while calculating the path on the basis of context of the nodes.

- Content Awareness – The proactive approach can be followed in routing in terms of content awareness. The particular path is chosen on the basis of the type of payload which needs to be communicated in the case of content-based routing [77]. The different type of data cannot be assumed as same. The requirements are different for the different type of data. And also, special consideration should be given to the type of data in IoT networks when it is to be transmitted on the noisy channel having low SNR. In paper [78], the authors mention that the text files are less delay tolerant whereas the audio and video files can tolerate the 30%-40% packet loss but not delay.

- Heterogeneity – In the above-mentioned table, the algorithms do not support heterogeneity. It is very alarming that the algorithms are not taking up the issue [74, 79-84]. The heterogeneity is a very big issue in IoT [92]. The heterogeneity is present in the IoT architecture at every layer and across the layer i.e. horizontally [85] and vertically. Recent algorithms are focusing in this area and the researchers are constantly working on it. There is wide variety of heterogeneity in IoT which is explained in detail in the next section.

### 3.5.2 Heterogeneity issues

The different types of Heterogeneity found in IoT networks are as follows.

- Communication Technology Heterogeneity: The variants in the communication technology make it difficult to communicate between the various nodes in the
routing path [43]. The technology which can be used in the communication can be Wi-fi, ZigBee, Near Field Communication (NFC), Bluetooth etc.

- Connecting Devices Heterogeneity: The communication path from the source to the destination is composed of various types of devices. From all these devices, the subset of devices when connected makes one routing path. There may be different neighboring nodes like mobile phones, access points, laptops and various types of other things like refrigerator, vacuum cleaner, geyser etc. in an IoT architecture. This may make switching difficult from one type of device to another type of device in the routing path [58,74].

- Topology Heterogeneity: Topology is the form of creation of network of connected things. The various types of topologies exist for IoT framework such as star, bus and mostly used is the mesh topology [80].

- Communication Range Heterogeneity: The communication range may be short or long in case of things connected under IoT ecosystem. The long-range communication may be carried through the short-range communications. Various devices are implemented with the long-range communication technology or the short-range communication technology depending on the type of communication [81].

- Addressing System Heterogeneity: The addressing system implemented and which is mostly used is IPv4 with 32-bit address space. But soon there will be shortage of addresses and soon we will be implementing IPv6 with 128bit address space to accommodate the increasing volume of things in the IoT networks [82].

- Data Heterogeneity: The data which can be transferred from a source to the destination can be any form such as text, audio, video or images. Depending on the context of the data or the content, the communication path may be chosen. Therefore, it is essential to know in advance, what kind of data we need to send to the destination [57].
All the types of Heterogeneity discussed above adds to the communication challenge of IoT. At every layer of the IoT architecture, the variety of smart devices, protocols, middleware, gateways etc. is seen. And the growth in IoT has been dependent on the standardization of the standards leading to the highest level of interoperability. The term interoperability can be defined as the capability to cooperate or interoperate between the various devices, systems and applications. The increase in the deployment of the wireless, smart objects, the network survival is a big challenge. And when the survivability also sees the heterogeneity [83] in the network, it becomes very important to address the issues as early as possible.

The co-existence of the wireless technologies is the high interest research area. The network layer faces these co-existence issues. Various things in the IoT network, may have different demands for the transmission range, transmission power, bandwidth requirements, storage requirements etc. Also, these smart things in the network would be having different QoS requirements such as speed, delay etc. The interoperability [84] can be there at four levels mentioned as following:

- **Technical Interoperability** - it mainly focuses on the hardware and the software systems, components and for the communication in the network. This is mostly required in case of the protocols used in the communication.

- **Symbolic Interoperability** - Different devices have different forms as provided by the different manufacturers and vendors. Common formats are required to deal with the syntax and encoding issues emerging from various protocols.

- **Semantic Interoperability** - It is related with the meaning of the information to be communicated in the network. The common understanding of the meaning is required and the semantic interoperability is application specific.

- **Organizational Interoperability** - It is possible when we have achieved interoperability at other levels successfully such as Syntactic, Semantic and Technical interoperability. It means communication should be effective through the organizations located anywhere, transferring any information using any infrastructure, gateways etc.

A high level of interoperability is required in the IoT networks.
3.5.3 Noise Issues

In WSNs the multimedia payload can generate a huge amount of data. The nodes in the WSNs are able to sense and communicate the multimedia content which can be streamed or considered as static image data. The WSNs are WSNs with multimedia capability. These networks are capable to transfer the multimedia content other than the scalar data. The multimedia content may include image, audio, video, text or their combination. The development in the technology such as WSNs, 5G networks, Wi-Fi networks has generated a huge demand for the multimedia applications. But the implementation of these applications demands the various QoS metrics to be maintained. The scope of these multimedia applications is very wide in case of IoT real time and non-real time applications. WMSNs are not limited to the IoT applications such as monitoring, smart cities etc. the QoS requirements such as multimedia data processing, end-to-end delay, bandwidth requirements, speed requirements etc. are application specific. The solutions to maintain these QoS requirements can be found by developing new protocols or by improving the current routing algorithms for the WSNs. To maintain the QoS in the multimedia, the real time networks pose more severe challenges. The different architectures, protocol stacks and constraints are to be followed in case of WMSNs and same cannot be followed in case of WSNs. The QoS requirements are also different in terms of bandwidth, delay, jitter etc. The delay limits are different and dependent on the type of the data to be communicated. The video data may hard real time and soft real time constraints where the delay limits are hard or flexible. The bandwidth consumed by the video data is higher as compared to the other types of data. The effective routing protocols are required for the WMSNs, as the traffic patterns are different in these networks and also the QoS factors are diverse for different kinds of data. Heterogeneous sensor data are there in multimedia applications at different data rate and may require additional QoS constraints to meet. More reliability is required in case of WMSNs as these networks generate highly uneven traffic, variable transmission data rates and high processing. The path selection scheme can be followed. It may be based on the type of the data. The path
is selected on the basis of the information stored in the packet header which is to be transferred.

The lifetime of the network is required to be increased, as the energy consumption of the nodes will be very high and the nodes may not be able to forward the data. Currently, the stress is being given on preserving the energy of the nodes and less focus is paid to reliable route discovery and the QoS requirements for the multimedia content.

It involves various kinds of data such as text, audio, video, image etc. The route from the source to the destination needs to be established based on the type of payload. The proposed algorithm CARA-IoT takes into consideration the type of data. The present routing algorithms are proving better results for the scalar data provided by WSNs but the same has still some challenges for the WMSNs multimedia content. The QoS has become a real challenge for such networks. There are various factors which affect the QoS such as delay, packet loss, jitter, congestion, SNR etc. The advancement in the technology field has led to the increase in the multimedia traffic and also in the routing challenges.

Several context aware algorithms have been proposed for the IoT networks. Along with these, the content aware routing algorithms are also required to deal with the various routing challenges of IoMT networks.

Various QoS metrics are:

- **PDR** - Packet Delivery Ratio
- **End-to End Delay**
- **SNR** - Signal Noise Ratio
- **Jitter**
- **Packet Loss Ratio**
- **Bandwidth requirements**
- **Data rate**
- **Energy consumption by the nodes**
Where Packet Delivery Ratio is defined as the ratio of the number of packets received by the receiver to the total number of packets sent by the sender.

\[
PDR = \frac{\text{No. packets received}}{\text{No. of packets sent}} \quad \text{Eq. (3.1)}
\]

The network performance is good if there is high PDR and vice versa.

End-to-End Delay is calculated as the time taken by the packet to reach from the source to the destination. The delay during the communication can be caused due to several reasons, may be through interference, queuing, packet conversions etc. It is actually the summation of transmission delay, queuing delay, propagation delay and processing delay. It is the time difference between the sending time and the receiving time of the respective packet. The network performance is good if the end-to-end delay is low and vice versa.

Types of content during Transmission: The payload to be transferred from the source to the destination can be of any form such as audio, video, image, text or it may be multimedia. And, also the audio or video data may not be in the same packet.

The different types of data can be in the form of audio, video, image, text or Multimedia – combination of any two or more of the any other type. The routing algorithms are required which are can find the reliable routes based on the content of the packets to be transmitted. The path’s reliability should be predicted and best route should be chosen to deliver the content. The path should be best in terms of delay, SNR, BER, PDR, throughput, speed, distance etc.

The challenges which can severely influence the growth of IoT are:

- Routing issues [22-42, 65-85]
- Heterogeneity issues [43-50, 57-58, 74-80, 84]
- Quality of Services (SNR issues) [51-64]

**3.6 Research Approach**

The proposed research in the thesis follows both conceptual as well as empirical approach. Primarily, the research has been conducted by performing literature
review to discover the IoT in detail, the protocol stack, the IoT architecture, the research issues and the current work done in the same domain. Then the conceptual and empirical research is conducted and the algorithms and solutions have been proposed. The simulator implements the algorithms and verifies the results. The results have been analyzed and the conclusion is drawn.

### 3.7 Research Objectives

Based on the research gaps in the literature review, the following objectives have been identified:

- **To conduct an intensive literature review and to analyze the various heterogeneity issues of the IoT networks.**

- **To propose and implement the swarm intelligence based routing algorithm that supports the heterogeneity of IoT.**

- **To propose a suitable content-based routing algorithm for delivering payloads in the noisy environment.**

- **To test all the proposed algorithms (above mentioned) and discover the best possible route for the payload delivery with the help of simulator.**
3.8 Proposed Work

The research gaps in the literature review give rise to several issues, which need to be resolved while developing and designing solutions for IoT networks. The thesis addresses to the routing problems of the current research in IoT. The researchers have followed various approaches while dealing with the routing and heterogeneity issues of these networks. The middleware approach has been used mainly in the current research but the work done in the thesis provides algorithms to deal with the major issues. The ACO, swarm intelligence-based principle has been applied to propose the solutions for routing and heterogeneity in IoT. The proposed algorithms Ant Colony Based Routing Algorithm for Heterogeneous IoT (ARAH-IoT) and Content Aware Routing Algorithm for IoT (CARA-IoT), find out the best reliable path, which takes into consideration the various vital routing metrics. The QoS is maintained and the process of routing has been proposed as simple, efficient and effective. The algorithms are compared with the standard algorithms and these are implemented on the simulator designed in C# (.Net Environment) – IoT Routing Simulator (IoTRSIm).

The study states that the current algorithms and the present simulators are not suitable enough to work in the IoT environment w.r.t routing and heterogeneity. The thesis mentions the need of the new routing algorithms and simulator which suffices for the requirements and finds more important parameters and proposes virtuous solutions.
Chapter 4

Swarm Intelligence Routing Algorithm based on Communication Technology Heterogeneity

As in the case of WSN and MANET, the nodes participating in the network are of same type. But the nodes in the IoT networks different technologies can be used such as Wi-fi, ZigBee and Bluetooth etc. Out of all the types of Heterogeneity discussed above, the paper focuses on the Heterogeneity which is due to the communication technology used by the various devices in the IoT networks. For supporting long range communications, the combination of all these technologies can be used. In that scenario, the routing becomes a real major challenge, as the data needs to travel different kinds of nodes.

In the Figure 4.1, the sample IoT network in emergency is given. A home enabled with the IoT devices is at fire. In the emergency situation, the smart device wants to communicate to the fire station. The fire station provides the fire truck as soon as the fire station gets the message. The smart device tries to connect the nearby devices such as vehicle, walking person, any other home network as seen in the
figure. The route is selected and the intermediate devices have different communication technology which makes the routing process tough and time is taken more. Time is a crucial factor when communication in emergency is required. It is very important to deal with the communication technology heterogeneity.

4.1 Different Technologies

The communication technology IEEE 802.11 (Wi-Fi), IEEE 802.15.4 (ZigBee) and IEEE 802.15.1 (Bluetooth) are the prominent short-range wireless communication technologies. Bluetooth can be used to send, audio, video, graphics etc. the ZigBee can be used to sense and control the wireless networks. Wi-Fi can be used for more stable wireless communication. This study primarily focuses on these three different kinds of technology while sending the payload from the source to the destination.

• Bluetooth
• Wi-Fi
• ZigBee

The Bluetooth standard (Figure 4.2) is based on the radio technology which makes the communication possible using radio waves in the network. It is mainly developed for the mobile phones but can be used for the short-range communication. It offers wireless communication, uses less power and very cost effective. It operates on 2.4 GHz frequency (unlicensed ISM band) which offers 720 kbps speed. The rest two technologies (Wi-Fi and ZigBee) can also operate on the same frequency band. Frequency Hop Spread Spectrum (FHSS) is used in case of Bluetooth where each channel is occupied for 62µs. The Bluetooth technology works on the topological principles of the piconet and the scatternet. A piconet may have 8 devices and can use point-to-point communication. This technology has several classes, which has different property-values for the range, output power etc. The Bluetooth technology has the following packet structure and protocol stack:
Likewise, the Wi-Fi is used for the stable connections as it provides short-range communication at higher data rate. WLANs are mainly formed using this technology. The devices can directly connect to the Internet or indirectly those can use the hot spots. It can also operate at 2.4GHz frequency band (unlicensed ISM band). And also uses both DSSS and FHSS spread spectrum technology. It also provides secure and reliable communication for the short-range as well. The Wi-Fi packet format is mentioned in Figure 4.3.

The devices in the sensor network are connected using ZigBee technology (Figure 4.4). Actual connection setup and the transmission is possible in case of ZigBee as compared Wi-Fi and Bluetooth, and also helps in power saving and the fast transmission. The two types of modes are possible in this technology, Beacon mode, where the coordinator in the network is battery powered whereas in the Non-Beacon mode, the coordinator in the network is main power supply. It also uses 2.4 GHz as Bluetooth (unlicensed band ISM). It mainly offers mesh topology in the network and multi-hop, reliable and self-organized routing.
The Table 4.1 mentions the various similarities and differences between the three technologies. It can be seen that the number of similarities is very less as compared to the number of differences between them. Although all the technologies can operate at the same frequency band i.e. 2.4 GHz and can be used for the short-range communication but the transmission range, transmission speed, packet formats etc. are all different.
There is much technological difference while considering the fact to transmit the payload in IoT as the devices may be Bluetooth, Wi-Fi or ZigBee enabled.

These cannot be assumed as same. The packets need to be communicated from one technology to the other. The conversion or switching between the technology does not come easy. It takes around 6.37 ms \[90\] (Figure 4.5) to convert the payload into the respective communication technology packet structure.
As seen in the figures of this chapter, all the communication technologies have different protocol stack, packet structure and frame format. Several approaches have been found in the literature survey such as gateway and middle-ware approach but these are not found fully suitable in case of IoT networks. This research finds it as a major issue and the algorithms are proposed to deal with the same.

**4.2 ARAH-IoT**

The ACO approach has been followed while proposing the algorithms for the communication technology heterogeneity. This swarm intelligence principle is used to find the optimal path for the payload delivery. The shortest route found is reliable, effective and efficient in terms of number of conversions to be made from one technology to the other, the time taken to reach the destination, higher throughput etc. The proposed algorithm ARAH-IoT is capable of providing all these features but also has some routing overhead due to the number of conversions of the packets from one technology to the other. This routing overhead can be ignored as it will be minimal, but provides a greater number of paybacks.

The FANT algorithm is used for the route discovery from the source to the destination but not vice versa. The best route in terms of number of conversions to be done, transmission power, transmission range is calculated by the forward ant. Once the forward ant reaches the destination, the rest of the forward ants are killed and the first forward is converted into the backward ant.

**Fig 4.5 Calculation of Conversion time in IDRA architecture [90]**

<table>
<thead>
<tr>
<th>Optimization</th>
<th>Avg execution time per packet (ms)</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDRA system overhead</td>
<td>1.28</td>
<td>20.09</td>
</tr>
<tr>
<td>Information management (Sect. 2.1)</td>
<td>0.59</td>
<td>9.26</td>
</tr>
<tr>
<td>Packet facade and packet identification (Sect. 2.2)</td>
<td>0.97</td>
<td>15.23</td>
</tr>
<tr>
<td>Aggregation (Sect. 3.1)</td>
<td>0.58</td>
<td>9.11</td>
</tr>
<tr>
<td>Protocol selection (Sect. 3.2)</td>
<td>0.02</td>
<td>0.31</td>
</tr>
<tr>
<td>QoS (Sect. 3.3)</td>
<td>0.51</td>
<td>8.01</td>
</tr>
<tr>
<td>Network protocols (CTP &amp; S-MAC)</td>
<td>2.42</td>
<td>37.99</td>
</tr>
<tr>
<td>Total overhead</td>
<td>6.37</td>
<td>100</td>
</tr>
</tbody>
</table>
This backward ant traverses from the destination to source and updates the routing tables at every intermediate node on the back traversal. The BANT visits all the intermediate nodes which were found by the FANT on the best route. The BANT updates the routing table with the value known as probability of goodness and reaches back to the source. The PoG can be found using the value of the path metric (which may be distance, delay etc.) from the destination to the first intermediate node. As the BANT traverses it takes 70% of the current edge and the 30% of the previous edges of the aggregate of the path metric.

### 4.2.1 Forward Ant Algorithm

**Step 1:** Select neighbor node which is within the transmission range of current node.

**Step 2:** If no path information available initially, broadcast FANTs to the neighbors of the current node. Else unicast the FANT to the best neighbor selected based on the value of PoG calculated using Equation 1.2

**Step 3:** Increment hop count value.

**Step 4:** If conversion of communication technology at the selected neighbor, set the conversion value=1 otherwise 0 and update its RT (Routing Table) with the following entries.

<table>
<thead>
<tr>
<th>FANT_ID</th>
<th>Source</th>
<th>Destination</th>
<th>Prev_Node</th>
<th>ConvY/N</th>
<th>Node_Type</th>
<th>HCount</th>
<th>Next_node Type</th>
</tr>
</thead>
</table>

**Step 5:** Check RT entry if next node is the destination. If Yes, move FANT to the next node, repeat step 4 and GOTO step 6.

Else, move FANT to the next node and repeat step 4.

**Step 6:** Stop

The route discovery is performed in the forward ant algorithm, from source node to the destination node. Initially hop count is zero and as the node traverses to the
destination, the hop count value is incremented. The algorithm checks if the conversions to be done is under range and also the hop count is under range and time to live for the ant is under range, it either broadcasts or unicasts the packet. If the destination is not found in the routing table of the neighbor node, it set the pheromone value to be 1 and broadcasts the ant otherwise unicast the ant. The best node is selected using the formula defined in Equation 1.1. And also, till the destination is found, whenever the communication technology changes, for every intermediate node, it increments the conv variable and after reaching the destination it calls the backward ant to update the path information.

4.2.2 Backward Ant Algorithm

Step 1: Convert the first FANT to reach the destination as BANT.

Step 2: Check RT entry of FANT visited for conv, hop count and distance values

Step 3: If conv=1, calculate convTime += conv*6.37

Step 4: Update the RT entry of neighbor for the time taken to reach the destination

Step 5: Visit the next neighbor stored in the RT of the current node.

Step 6: If the next node is the source, update the pheromone value (consider distance, hop count and conversion time) at source RT and GOTO step 5

Else, repeat step 2 and apply 70%-30% rule for 70% of the current pheromone value and the 30% of the previously calculated pheromone value.

Step 7: Update the RT values

BANT_ID Source Destination Pheromone_value

Step 8: Stop pheromone calculation process

4.2.3 Packet Delivery Algorithm

Step 1: Start packet delivery process

Step 2: Check source node RT for the pheromone values and the PoG values of the neighbor nodes.
**Step 3:** Calculate PoG values using:

\[ \text{PoG}(A) = \frac{\text{Ph}(A)}{\text{Ph}(B) + \text{Ph}(C) + \text{Ph}(D)} \]  
(where B, C and D are the immediate neighbors of source A)

**Step 4:** Start packet delivery through the best selected path having highest PoG value

**Step 5:** Send all the packets using the chosen path till 100% delivery including retransmissions

**Step 6:** Stop packet delivery process

Initially the pheromone value is 0 and during the backward traversal from destination to the source node the hop count and conv variables are incremented. The total conversion time is calculated as no of conversions multiplied by 6.37 ms. Routing tables are updated using the equations and if the node is traversed again, the fitness value is calculated which takes the 70% of the value of the current edge and the 30% of the whole path from the source to the destination.

The ACO has been always used for finding the shortest reliable route based mainly on the distance between the sender and the receiver on the communication channel. According to the literature survey, the algorithms which are based on ACO find best routes for the optimization problems. The ARAH-IoT and the CARA-IoT are proposed algorithms based on the ACO approach and are modified according to the proposed study taking various other parameters which were not considered in case of ACO such as communication technology heterogeneity, speed, delay etc. The working principle of FANT and BANT have also been explained in chapter 6 and the flowcharts are as follows.
Fig 4.6 FANT working for ARAH-IoT
Fig 4.7 BANT working for ARAH-IoT
Chapter 5

Swarm Intelligence Based Routing Algorithm to Deal with Data Heterogeneity

5.1 SNR

Noise in the channel is very important to be considered. The noise means the unwanted signals or the interference due to any reason. The path which has less noise should be considered as it will be more reliable. Basically, WMSNs are focused on real time multimedia transmission in the networks. In these networks, the QoS [93] becomes a real challenge while traversing multipath routing protocols. If the route has higher SNR, it means that the strength of the signal is more as compared to the noise on the channel and if the SNR is low, it means the signal strength is less as compared to the noise [94,99-100]. It is always the high SNR which is preferable.

It is said that the pure signal does not exist. It means that the pure signal is termed as the signal which is noise less or noise free. But when we want to transmit the data, we require the pure signal, but as it is not possible, we can have the signal which is less affected from the noise.

The BER can be calculated from the SNR value, which further can be taken to calculate the goodness of the route.

\[ \text{BER} = \frac{1}{2}(\text{SNR}) \]  

Eq. (5.1)

The BER is the bit error rate which means the number of bits with errors to the total number of bits sent in the transmission. The relation between the SNR and the BER is opposite. The high value of SNR results in less BER and the low value of SNR means high BER.

The reliable results can be found if the SNR is high. The algorithm CARA-IoT is proposed which is takes into consideration the noise on the channel. And using
ACO approach, CARA-IoT is applied to find the reliable path which is best in terms of distance, speed, transmission range, noise, packet delivery ratio and throughput. Maximum number of QoS metrics are considered and the CARA-IoT is implemented. The IPv6 packet structure [96] is mentioned as below (Figure 5.1)

<table>
<thead>
<tr>
<th>Version</th>
<th>Traffic Class</th>
<th>Flow Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload Length</td>
<td>Next Header</td>
<td>Hop Limit</td>
</tr>
<tr>
<td>Source Address</td>
<td>Destination Address</td>
<td></td>
</tr>
</tbody>
</table>

**Fig 5.1 IPv6 Packet**

The above fig 5.1 is the IPv6 packet structure where a packet means the combination of the packet header and the payload. The fields of the packet structure are explained as under:

- **Version** – it is 8bit field explaining the version of the Internet Protocol
- **Traffic class** – it is also 8bit field to explain the different priorities and classes of the traffic
- **Flow Label** – it is 20bit field to mention the label sequence of the packets for the forwarding routers in the network and also allow request for the special handling of the packets
- **Payload** – it is 16bit unsigned integer to represent the payload. Except the header, rest in the packet is noted as payload including any extension headers if any
- **Next Header** - it is also 8bit header, which is for the next intermediate node in the route
- **Hop Limit** – it is also 8bit long, which checks for the number of hops to be visited to reach the destination and works in the reverse manner i.e. decremented by one every time the node is visited
- **Source Address** – it is 128 bit long to mention the source address
- **Destination Address** – it is also 128 bit long to mention the destination address.
The above packet can be used according for the communication of the multimedia content in the network. The field Traffic class of the packet structure may contain the following values depending on the content of the packet:

- Image data – 0000
- Video data – 0001
- Text data – 0010
- Audio data – 0011
- Multimedia data - 0100

And also, the flow label field of the packet structure contains the value for the sensitivity or priority of the data. For instance, if the data is normal snapshots, the value can be 00 whereas if the data is real-time video streaming for remote health monitoring, the value can be 01.

- Sensitive image data – 0000
- Normal image data – 0001
- Sensitive video data – 0010
- Normal video data – 0011
- Sensitive text data – 0100
- Normal text data – 0101
- Sensitive audio data - 0110
- Normal audio data – 0111
- Sensitive multimedia data – 1000
- Normal multimedia data - 1001

The paper [97] mentions the following points regarding different types of data to be communicated on the network. The delay which can be considered for different data is mentioned in Table 5.1. In [98], the authors mention that even the delay of 150 ms was not acceptable during some experiments.

As the delay requirements are different for the different kinds of content to be delivered. There is need to choose the best reliable routing path in multipath routing.
scenarios [91]. According to the requirement, the path may be chosen such as:

- Path A may be chosen if the content is Image
- Path B may be chosen if the content is Text
- Path C may be chosen if the content is Video
- Path D may be chosen if the content is Audio
- Path E may be chosen if the content is Multimedia

Content based choice for the path is required to be made. For instance, Path A, may not prove reliable for the textual content to be delivered reliably. That may be more error prone. The reliability of the path must be checked in advance before delivering the context. Before the transmission gets started, the PoGoM [42] of the path should be known to get the best delivery results in terms of delay, error, retransmission etc.

### Table 5.1: Acceptable delay limit for different type of content on wireless channel [97]

<table>
<thead>
<tr>
<th>Content Type</th>
<th>Acceptable Delay Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Textual Data</td>
<td>2-5 Sec</td>
</tr>
<tr>
<td>Audio data</td>
<td>Less than 600 ms</td>
</tr>
<tr>
<td>Video data</td>
<td>Delay should not exceed 250ms</td>
</tr>
<tr>
<td>Image data</td>
<td>155 ms</td>
</tr>
</tbody>
</table>

According to the literature survey, the metrics which can be used for the comparison of the various algorithms are packet delivery ratio, throughput etc. The proposed algorithm CARA-IoT takes into consideration all the parameters such as distance, technology conversion time (because of heterogeneity), speed, delay on the channel, packet drop and calculates the packet delivery ratio and throughput. CARA-IoT finds the best reliable path taking all these parameters into consideration which were not considered in case of ACO approach.

### 5.2 CARA-IoT
5.2.1 Forward Ant Algorithm

Step 1: Select neighbor node which is within the transmission range of current node

Step 2: If no path information available initially, broadcast FANTs to the neighbors of the current node
Else unicast the FANT to the best neighbor selected based on the value of PoGoM calculated using Equation 1.2

Step 3: Increment hop count value

Step 4: If conversion of communication technology at the selected neighbor set the conversion value=1 otherwise 0

Step 5: Check for Noise in the channel. Calculate SNR and BER using Equation 5.1 and update its RT (Routing Table) with the following entries

FANT_ID Source Destination Prev_Node ConvY/N Node_Type HCount Next_node Next_Node_Type Noise Y/N

Step 6. Choose the neighbor based having lesser number of packet drops

Step 7: Check RT entry if next node is the destination. If Yes, move FANT to the next node, repeat step 4 and 5 and GOTO step 8
Else, move FANT to the next node and repeat step 4,5 and 6

Step 8: Stop

5.2.2 Backward Ant Algorithm

Step 1: Convert the first FANT to reach the destination as BANT

Step 2: Check RT entry of FANT visited for conv, hop count and distance values

Step 3: If conv=1, calculate convTime += conv*6.37
If Noise = ‘y’, calculate delay on the channel

Step 4: Update the RT entry of neighbor for the time taken to reach the destination

Step 5: Visit the next neighbor stored in the RT of the current node
Step 6: If the next node is the source and update the pheromone value (consider distance, hop count and conversion time and noise on the channel) at source RT and GOTO step 5

Else, repeat step 2 and apply 70%-30% rule for 70% of the current pheromone value and the 30% of the previously calculated pheromone value

Step 7: Update the RT values

BANT_ID Source Destination Pheromone_value

Step 8: Stop pheromone calculation process

5.2.2 Packet Delivery Algorithm

Step 1: Start packet delivery process

Step 2: Check source node RT for the pheromone values and the PoGoM values of the neighbor nodes

Step 3: Calculate PoGoM values using:

\[ P_{GoM}(A) = \frac{P_A}{P_B + P_C + P_D} \] (where B, C and D are the immediate neighbors of source A)

Step 4: Check the delay value in all the PoGoMs for the type of packet to be transmitted as given in the table 5.1

Step 5: Start packet delivery through the best selected path having highest PoGoM with the lowest delay value

Step 6: Send all the packets using the chosen path till 100% delivery including retransmissions

Step 7: Stop packet delivery process
Fig 5.2 FANT working for CARA-IoT
Fig 5.3 BANT working for CARA-IoT
Chapter 6

Simulator

6.1 Introduction to IoTRSim

The simulator IoTRSim, has been designed and developed in C# (.Net environment). In the previous chapter of this dissertation, the need of developing new simulator has been explained.

The below image provides the interface of the simulator IoTRSim. Like the standard simulators, the properties of the nodes have been considered and taken care of. The properties of the sensor nodes considered in the simulator are communication technology heterogeneity (ZigBee, Bluetooth and Wi-Fi), the transmission range of the nodes, the percentage drop in the speed of the nodes, the conversion time taken for converting one technology to the other, the accepted delay limits for the different type of content and also the distance between the nodes.

Also, for calculating the probability of goodness of the routing path for the payload transmission, the ant properties also taken such as no. of ants and no. of iterations in the simulation.

The different type of nodes can be taken for the simulation purpose, also, we can enable specific types of nodes according to the requirements. The default values taken are conversion value as 6.37 ms, packet size as 512 kb, the delay limit for text as 5 sec, the delay limit for image as 155 ms, the delay limit for audio as 600 ms and for video as 250ms. The simulator works on the ACO principle after taking all these values. The nodes can be plotted randomly and different comparison charts can be prepared from the data captured. The simulator captures the data for every run and the data is stored and appended in the text file and the graphs are made accordingly.
The variable values can be taken for the following properties:

- No. of ants
- No. of nodes
- No. of iterations
- Payload size – size varies according to the content uploaded
- Node speed
- Packet drop percentage
- Packet drop range limit
- Node speed full range limit

The assumptions are made for the packet drop percentage and also for the delay at the particular node to be computed at the runtime. The pheromone value of the ants calculates the PoGoM and updates the routing entries. The pheromone is calculated on the basis of conversion time, speed of the device technology, packet drop and also the distance between the nodes.
The developed simulator IoTRSIm provides the flexibility to provide the values. So, it is easily configurable. It works on the values provided. Different values can be provided for the different simulation scenarios. The user can set the values according to the environment needs.

Based on the provided metrics, the proposed algorithms, ARAH-IoT and CARA-IoT, are compared with the standard algorithms and the results are analyzed. The graphs are generated for the comparison on the basis of packet delivery ratio, total distance travelled, total time taken to reach the destination including conversion time, end-to-end-delay and throughput.

The next image (figure 6.2) shows the IoTRSIm simulation after implementing the proposed algorithms:

![Sample IoTRSIm Simulation](image.png)

Fig 6.2 Sample IoTRSIm Simulation

The Figure 6.2 shows the sample run. This simulation is carried out for the upload of image file. The best reliable routing path is calculated based on the shortest distance possible considering packet delay at every node, nodes transmission range,
the speed of the node and also the conversion time taken. It can be seen in the image that best route is covering more distance than the standard ACO approach, still it has taken the lesser time and is better in terms of delay, packet delivery ratio and throughput. Such simulations have been carried out for the no. of nodes ranging from 10-50 and for the following simulation parameters.

6.2 How FANT and BANT works for the ARAH-IoT and CARA-IoT

FANTs are moved from node A to node B (Figure 6.3), node J and node E. Initially it broadcasts as it does not have prior information about the goodness of the nodes and the path. Likewise, FANTs are moved and allowed to reach the destination. The first FANT which reaches the destination node D is changed into BANT and all the rest of the FANTs are killed. In between the route discovery process, if the Ants’ time to live get expired or if maximum hop limit is reached, the FANT is killed.

The BANT takes the value of the metric into consideration for calculating the probability of goodness of the path. The metric which can be used for the calculation may be distance, delay, hop count etc. In the proposed algorithms in this
study, the primary metric to be considered are conversion time in case of ARAH-IoT and transmission speed of the nodes and noise (SNR, BER) in case of CARA-IoT (Figure 6.4).

Suppose that Path 1 is chosen to be the most reliable and best route from node A to node D, then the BANT moves from node D to node C and update the routing table stored at node C as 70% of value 10 and then BANT moves from node C to node B and update the routing table stored at node B to value calculated as 30% of value 10 plus 70% of DC edge value. The same procedure is applied from node B to node A.

Now except initial run, the values of PoG and PoGoM (in case of CARA-IoT) are stored in the routing table of A. whenever the packet is to be transferred from the node A to node B, the FANT checks for the routing table entry and compares the probability of goodness of all its neighbor. The highest value of PoG and PoGoM (in case of CARA-IoT) is chosen and FANT is moved to that chosen neighbor only. The provision for the pheromone evaporation is also made, so that to avoid only one route for the transmission.

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric Value (Distance)</th>
<th>PoG</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>3</td>
<td>0.8</td>
</tr>
<tr>
<td>J</td>
<td>8</td>
<td>0.3</td>
</tr>
<tr>
<td>E</td>
<td>5</td>
<td>0.6</td>
</tr>
</tbody>
</table>

Now the routing table (Table 6.1) entry clearly shows that node B will be chosen as the next intermediate node from node A. and again in the next cycle, the routing tables are updated stored at the intermediate nodes by the BANT.
In the Figure 6.4 there is more noise on the path 1 on the nodes from node B to node C.

And there is less noise on the path 3 from node H to node I. The algorithm CARA-IoT chooses the path 3, because despite having a greater number of intermediate hops in between from source to destination, it is having least noise.

The CARA-IoT algorithm, takes care of the SNR, BER, speed of the nodes, transmission range of the nodes, distance, delay, conversion factor and applies the ACO principle as mentioned above for the ARAH-IoT algorithm. It then calculates the best reliable route from source node A to the destination node D. As in the Figure 6.4, the best reliable route is from A-F-G-H-I-J-D.

The Figure 6.5 is of the text file which is automatically created when the network is created in the simulator IoTRSIm and allowed to run. The values are captured and the results are computed and the graphs are drawn. It automatically creates the log of the simulation and appends in the file as soon as the simulation gets stopped.
Route Log 10 3/19/2019 11:14:20 PM
CARA-IoT Distance 341.52
Average Speed
1-3-33.25
3-6-4.17
6-10-7.49
CARA-IoT Full node speed
1-3-75
3-6-20
6-10-42
CARA-IoT Node Time
1-3-71.6950367107195
3-6-571.804482446245
6-10-318.33997377566
CARA-IoT Node Packet Delivery Time
1-3-0.02
3-6-0.12
6-10-0.07
CARA-IoT Node Time Conversion Time
1-3-0.1
3-6-0.6
6-10-0.32
Node Time Conversion 1.02
ACO Best Distance 341.34
ACO Node Time
1-6-893.51
6-10-318.34
CARA-IoT Node Time- 1211.85
ACO node conversion time 0
CARA-IoT HopCount 2
ACO HopCount 1
Drop %
1-0
2-0
3-0
4-0
5-83
6-16
7-17
8-12
9-15
10-15
Delayed node time
1-4-161.91

Fig 6.5 Log File Route.txt-Sample
Chapter 7

Results and Analysis

7.1 Simulation Environment

The IoTRSIm simulator has implemented various scenarios where nodes were randomly placed and the results are calculated.

The simulation table (Table 7.1) mentions the parameters taken for the implementation of the ARAH-IoT algorithm. It takes into consideration the various parameters like the no. of nodes used for the simulation, no. of ants for calculating the reliable path out of all the available paths, no. of iterations to calculate the precise and accurate result i.e. best path, the ZigBee enabled node with the speed as 75 Mbps for the ZigBee transmission range assumed as 75mtrs, where the packet drop percentage due to noise is assumed as 25 % for every 15 mtrs. Likewise, the values are taken for the Bluetooth enabled node and the Wi-Fi enabled node. The Bluetooth node speed is assumed as 20 Mbps for the range 10 mtrs and the packet drop is assumed as 10% for every 5 mtrs. And the Wi-Fi node speed is assumed as 50 Mbps for the range 50 mtrs and the packet drop percentage is taken as 15% for every 10 mtrs.

The payload size in the packet is taken as 100 mb and the most important metric to be considered in this algorithm is the conversion time, which is 6.37 ms. It is the time which a node takes to convert the packet, if the packet received is not of the same technology as that of the receiving node.

Likewise, the Table 7.2 is mentioned for the implementation of the CARA-IoT algorithm. It takes all the values of ARAH-IoT implementation and has the added features such as delay limits or the acceptable noise limits for the various kinds of the data.
The simulation environments are mentioned as following.

Table 7.1 Simulation parameters based on ARAH-IoT

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Area</td>
<td>500m x 500m</td>
</tr>
<tr>
<td>No. of Nodes</td>
<td>10-50</td>
</tr>
<tr>
<td>No. of Ants</td>
<td>10-50</td>
</tr>
<tr>
<td>No. of Iterations</td>
<td>10-20</td>
</tr>
<tr>
<td>ZigBee Speed</td>
<td>75 mbps (full range is assumed to be 75m) with percentage drop of 25% for every 15m</td>
</tr>
<tr>
<td>Bluetooth Speed</td>
<td>20 mbps (full range is assumed to be 10m) with percentage drop of 10% for every 5m</td>
</tr>
<tr>
<td>Wi-fi Speed</td>
<td>50 mbps (full range is assumed to be 50m) with percentage drop of 15% for every 10m</td>
</tr>
<tr>
<td>Conversion Factor</td>
<td>6.37 ms</td>
</tr>
<tr>
<td>Payload Size</td>
<td>100MB</td>
</tr>
</tbody>
</table>

Table 7.2 Simulation parameters based on CARA-IoT

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Area</td>
<td>500m x 500m</td>
</tr>
<tr>
<td>No. of Nodes</td>
<td>10-50</td>
</tr>
<tr>
<td>No. of Ants</td>
<td>10-50</td>
</tr>
<tr>
<td>No. of Iterations</td>
<td>10-20</td>
</tr>
<tr>
<td>ZigBee Speed</td>
<td>75 mbps (full range is assumed to be 75m) with percentage drop of 25% for every 15m</td>
</tr>
<tr>
<td>Bluetooth Speed</td>
<td>20 mbps (full range is assumed to be 10m) with percentage drop of 10% for every 5m</td>
</tr>
<tr>
<td>Wi-fi Speed</td>
<td>50 mbps (full range is assumed to be 50m) with percentage drop of 15% for every 10m</td>
</tr>
<tr>
<td>Delay Limit</td>
<td>As mentioned in Table 1</td>
</tr>
<tr>
<td>Payload Size</td>
<td>Content Based–Text/ Audio/Video/Image/Multimedia</td>
</tr>
<tr>
<td>Packet Transmission Size</td>
<td>512 KB</td>
</tr>
</tbody>
</table>
7.2 Results based on ARAH-IoT

It has been seen that ACO approach performs better in case of routing protocols. So, it has been used in the proposed algorithms with new metrics. And it is seen that the proposed algorithm ARAH-IoT performs better than standard ACO approach.

As in the Figures 7.1 and 7.2, it can be seen that the distance covered by the ARAH-IoT is more, still it is taking less time to reach the destination, which is a very crucial factor in case of routing.
The simulation has been performed for varying number of nodes. The graph (Figure 7.3) shows that the number of hops visited in the simulations may be more in case of ARAH-IoT.

Also, it can be seen that the number of conversions is taken proper care of in case of ARAH-IoT and the path is chosen on the basis of number of conversions in the path so that the conversion time should be less while reaching the destination.
7.3 Results based on CARA-IoT

The simulator algorithm for considering the noise on the channel and for considering the type of payload, the CARA-IoT when compared with the standard ACO algorithm, performs better in terms of several parameters. The CARA-IoT is the extension of the ARAH-IoT algorithm which additionally considers noise and type of payload for transmission in multimedia networks.

Fig 7.5 ACO vs CARA-IoT (Distance)

Both the Figures 7.5 and 7.6 show the performance level of CARA-IoT, even when the distance covered by the CARA-IoT algorithm is more, the time taken is less to reach the destination, as it was in ARAH-IoT.
The packet delivery ratio (Figure 7.7) is more in case of CARA-IoT when compared with the ACO algorithm. It may be sometimes less, but the speed offered by CARA-IoT is very high.

The figure shows that the average speed comes out to be impressive in case of CARA-IoT as compared to the standard algorithm ACO. Speed factor is very crucial in case of reliable routing.
7.5 Results based on different simulations

The graphs show the sample run for the different number of nodes such as 10, 20, 30 etc. The graphs are mentioned for the different QoS parameters such as PDR, No. of Conversions, distance, hop count etc.

Fig 7.9 IoT network with 10 nodes

Fig 7.10 CARA-IoT vs ACO on the basis of distance (10 Nodes)
The distance (Figure 7.10) covered by CARA-IoT is more than the ACO, still it gives more speed for the transmission of the payload.

Fig 7.11 CARA-IoT vs ACO on the basis of hop count (10 Nodes)

The no. of hop counts (Figure 7.11) and the conversion time (Figure 7.12) is also more in this case of simulation for CARA-IoT as compared to the ACO.

Fig 7.12 CARA-IoT vs ACO on the basis of conversion time taken (10 Nodes)
Fig 7.13 CARA-IoT vs ACO on the basis of average speed (10 Nodes)

The speed offered (Figure 7.13) by the CARA-IoT is much more as compared to ACO and also the end-to-end delay (Figure 7.14) is very less.

Fig 7.14 CARA-IoT vs ACO on the basis of end-to-end delay (10 Nodes)
Fig 7.15 CARA-IoT vs ACO on the basis of throughput (10 Nodes)

The PDR (Figure 7.16) is little less in CARA-IoT but the throughput (Figure 7.15) is very high in case of the CARA-IoT as compared to ACO.

Fig 7.16 CARA-IoT vs ACO on the basis of packet delivery ratio (10 Nodes)
Similarly, the following graphs mention the simulation runs for varying number of nodes (15, 20 and 25) of CARA-IoT and the better performance of the algorithm in comparison to ACO.

**Fig 7.17 IoT network with 15 nodes**

The Figure 7.17 shows the IoT network simulator with 15 nodes.

**Fig 7.18 CARA-IoT vs ACO on the basis of distance (15 Nodes)**
It can be seen clearly that (Figure 7.18, 7.19, 7.20 and 7.24), the distance covered, hop count and conversion time are high in case of CARA-IoT and also PDR is slightly low but the average speed (Figure 7.21) and the throughput (Figure 7.23) of the network following CARA-IoT are very high than the ACO and also the end-to-end delay (Figure 7.22) is also minimized using the CARA-IoT algorithm.

Fig 7.19 CARA-IoT vs ACO on the basis of hop count (15 Nodes)

Fig 7.20 CARA-IoT vs ACO on the basis of conversion time taken (15 Nodes)
Fig 7.21 CARA-IoT vs ACO on the basis of average speed (15 Nodes)

Fig 7.22 CARA-IoT vs ACO on the basis of end-to-end delay (15 Nodes)
Fig 7.23 CARA-IoT vs ACO on the basis of throughput (15 Nodes)

Fig 7.24 CARA-IoT vs ACO on the basis of packet delivery ratio (15 Nodes)
It can be clearly seen in the Figures 7.26, 7.27, 7.28 and 7.32 that despite covering more distance, higher number of ho counts, no. of conversions and slightly low PDR, the algorithm CARA-IoT offers very throughput (Figure 7.30), higher average speed (Figure 7.31) and very low end-to-end delay (Figure 7.29) as compared to ACO with 20 nodes.
Fig 7.27 CARA-IoT vs ACO on the basis of hop count (20 Nodes)

Fig 7.28 CARA-IoT vs ACO on the basis of conversion time taken (20 Nodes)
Fig 7.29 CARA-IoT vs ACO on the basis of end-to-end delay (20 Nodes)

Fig 7.30 CARA-IoT vs ACO on the basis of throughput (20 Nodes)
Fig 7.31 CARA-IoT vs ACO on the basis of average speed (20 Nodes)

Fig 7.32 CARA-IoT vs ACO on the basis of packet delivery ratio (20 Nodes)
As seen in the previous graphs, it can be seen in the Figures 7.34, 7.35, 7.36, that the distance covered, no. of hop counts and no. of conversions are higher in case of CARA-IoT even then the average speed (Figure 7.37), throughput (Figure 7.39), PDR (Figure 7.40) are very high and also the end-to-end delay (Figure 7.38) is very low with 25 nodes.

Fig 7.33 IoT network with 25 nodes

Fig 7.34 CARA-IoT vs ACO on the basis of distance (25 Nodes)
Fig 7.35 CARA-IoT vs ACO on the basis of hop count (25 Nodes)

Fig 7.36 CARA-IoT vs ACO on the basis of conversion time (25 Nodes)
Fig 7.37 CARA-IoT vs ACO on the basis of Average Speed (25 Nodes)

Fig 7.38 CARA-IoT vs ACO on the basis of End-to-End Delay (25 Nodes)
Fig 7.39 CARA-IoT vs ACO on the basis of Throughput (25 Nodes)

Fig 7.40 CARA-IoT vs ACO on the basis of PDR (25 Nodes)
Chapter 8

Conclusion and Future Scope

The dissertation considers the solutions for the crucial issues of the IoT networks. The IoT is the progressing field and is expected to grow at exponential rate. The sensor devices are already common now and we can find those at homes and offices easily. But there is lacking support for the communication of these sensor smart devices without human intervention. The benefits of the IoT will only be tasted, if we are able to resolve the issues related with IoT as soon as possible. The study presents the several issues emerging from this field. Most important are found to be related with routing and heterogeneity in IoT networks. The important metrics should be given due importance such as end-to-end delay, packet delivery ratio, throughput, signal noise ratio etc. Also, the heterogeneity is found to be at maximum in case of IoT networks. The research presents various types of heterogeneity and analyzed that most important are communication technology heterogeneity and data heterogeneity. Several issues have been found, while dealing with these both. The dissertation proposes the algorithms for the reliable routing and for resolving heterogeneity issues of IoT architecture. ACO approach has been used for finding the reliable routing solutions. According to literature survey ACO approach has been found that the proposed algorithms are performing better than the standard algorithms in terms of throughput, average delay, packet delivery ratio etc. The algorithms are tested and implemented on the simulator which is designed in C# (.Net platform). As the standard simulators are studied and analyzed these are not found suitable at present for providing solutions for routing and heterogeneity issues of IoT networks. That is why, own simulator IoTRSim has been developed with the vital node metrics required for the simulation purpose. The results show that there has been more than 200 % increase in the speed using the proposed algorithms and more than 50% decrease in case of end-to end delay. It can be concluded that using such approach and the proposed simulator and algorithms, the solutions can be found for the IoT network issues.
Future Scope

The researchers are continuously working in this domain. The research is going at very fast pace and the solutions have been found for most issues. The future work can be done on the different technologies. The proposed simulator’s functionality can also be improved in the future to include the live video streaming. The efforts can be made to propose a single format so that the conversion to the different technology (of the sensor device) can be avoided. All the smart sensor devices should follow only one format whether it be ZigBee, Wi-Fi or Bluetooth. We can avoid the conversions, delays and the gateway approach. More simple solutions can be found avoiding routing overheads. Also, the IoT architecture may be changed and instead of having only three prominent layers, we can have one more layer, which does all the necessary modifications. Along with the routing and heterogeneity issues, there are several other such as privacy, maintaining security of data etc. Some algorithms may be proposed by the researchers, which take into account all these together (heterogeneity, privacy, security, etc.).

The transmission of multimedia content is possible today, but fast transmission of the data is required. The researchers may work for the processes for fast delivery of data which takes less time and effort and the energy of the nodes is also saved. Algorithms are also required for the management of node failure and saving the energy of the smart devices. When all these issues are taken care of, it will not take much time to change this world of devices. Soon we will be having a greater number of smart devices communicating with other efficiently and effectively without the need of human intervention.
References


