CHAPTER 6

ASPECTS OF TRUSTED ROUTING COMMUNICATION IN SMART NETWORKS

In this chapter, we have exploited the WTR mechanism to detect and eliminate the malevolent/malicious nodes involved during the routing path formation for smart-home environments where the routing between the communicating entities is performed through the mesh architecture. In order to provide a secure communication against malicious behavior of nodes, the proposed mechanism uses Dijkstra’s shortest path routing algorithm in which the weights are deliberated using certain parameters such as node distance, packet-loss percentage and trust value of each node which is computed using SITO. Further, we have discussed the network performance trade-off caused by secure path formation with conventional method and have proposed the WTR mechanism for eliminating the potential issues such as packet-loss ratio, end-to-end delay and network throughput. The NS2 simulator is used to simulate and compare the network metrics for both conventional and the proposed approach and is validated through experimental results over end-to-end delay and message delivery ratio against reported literature.

6.1 INTRODUCTION

With the recent societal development, the demand of digital environments where humans interact smartly with their surroundings to increase their comfort zone as compared to the hard build infrastructures is accumulating day by day. Smart cities, smart homes and smart societies are potentially hot trends of intelligent environments where multiple internet-of-things (IoT) devices respond as human behavior by automatically controlling and adapting the environmental situations [118, 119]. In order to provide the interconnectivity among the communicating entities or to enhance the coverage area by introducing additional placements of devices, there is a need to use a more efficient, robust and reliable communication standard such as Zigbee, Bluetooth or Wi-Fi [120, 121]. Currently, for such systems, Zigbee is one of the most widely used wireless technology because of its mesh based architecture which allows high scalability (because of its multi-hop feature) and provides large coverage area by incorporating self-healing, self-organizing and self-configuring characteristics [122, 123].
Although, the main stream of such systems is to achieve a seamless integration of intelligent sensing and networks to provide an automated life. However, the equally important issue of handling the security in these environments is not reported in depth where the inter-connection between the devices is subject to a number of security threats either from remote attackers or from inside home area networks. The most important factor that impacts the security is the nature of fundamental routing protocols used for promoting the message signals [124-126] where the presence of any malicious or misbehaving node within the routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network. The smart devices acquire a vast amount of sensitive data whose collection and processing raises several privacy concerns regarding the secrecy of the data that would be shared only for their own good rather than being collectively or maliciously disclosed for the purpose of violating their autonomy and privacy [127, 128].

The conventional routing protocols operate smoothly with an assumption that all the intermediate nodes are trusted and cooperative with each other. However, the dynamic and multi-hop features of the mesh network invite a number of internal vulnerabilities to come where attackers may launch several types of attacks either by compromising the legitimate routing nodes or by disrupting the data packets [129-131]. Therefore, one of the norm approaches to counter such attacks is secure routing. Most of the previously proposed approaches use cryptographic operations to ensure the integrity and confidentiality of the nodes using trusted third party. The issue with these techniques is that they seems to be infeasible in mesh environments (because of its broadcasting and dynamic nature) due to certain parametric issues such as computational, communication and storage overheads. Further these techniques are effective for external attacks and are found completely infeasible to ensure the security against internal threats [132]. Recently, the trust based methods have suit an active research area as they have emerged as a viable solution to take the routing decision and overcome the above discussed issues. A number of trust based methods have been proposed for MANETs, WSNs [133, 134] and other networks [135, 136] that are basically espouse for homogenous systems and cannot be adapted well in heterogeneous mesh networks because of their multi-hop and dynamic nature [137-138]. Therefore, there is a need to provide a secure communication mechanism that overcomes the computational, communication and storage issues and ensures efficient routing procedures for establishing the communication in smart home environments.
In this chapter, a trusted weight computation through SITO mechanism is proposed for smart home communication procedures that is based on mesh architecture and ensures a secure path formation in the network by detecting and eliminating the malicious nodes. Further, the Dijkstra’s shortest path routing algorithm is used to route the data packets to yield the shortest way between the communicating entities [139]. The Dijkstra’s algorithm is chosen for the purpose due to its lesser computational complexity as compared to other shortest path routing algorithms such as bellman ford algorithm used by Khan et al. [140, 141] to explore their secure approach. Further, it considers positive weights to avoid the loop formation process. While the greedy algorithms like greedy parameter circuit routing (GPCR) algorithm does not provide the accurate measurements and must be tested on similar environments where their results should be compared with the existing approaches again and again. The potential contribution towards a secure routing mechanism is summarized as follows.

- The Dijkstra’s shortest path routing algorithm is used to yield the shortest path between the communicating entities whose weights are assigned according to their trust factor which is computed using certain factors i.e. node distance, trust of a node, residual energy and packet loss ratio.
- The simulations are performed using commercial simulator NS2 and are experimentally validated over real environment to analyze and evaluate the network metrics against reported SRPM protocol that is considered as the basic approach of our chapter [142].
- The behavior of both the protocols is first analyzed under small network sizes and then under large network sizes having fixed number of nodes against different network metrics. Further the network metrics are measured under scalable network sizes in mobile nature where the nodes are moving at the speed of 0-25 m/s and the proposed protocol is validated under various adversary nodes having two different scenarios (metrics are measured against two severe routing attacks i.e. black hole and falsification attacks over scalable network sizes, and the performance is checked by increasing the number of black hole and falsification nodes near source and destination over small and large network sizes). A black hole attack is the one in which the compromised or malicious node offers itself as the shortest route to reach the destination so that it can drop the entire packet flow going towards it while falsification is the attack where an intruder hacks the legitimate node’s address with the aim of affecting the performance metrics of the network. These two attacks are taken as two severe routing attacks because they drastically affect the
network performance. Moreover, the experimental results are shown for end-to-end delay and Message Delivery Ratio (%) for both the approaches.

The remaining structure of the chapter is organized as follows. Section 2 describes the related work reported by various researchers. The proposed WTR mechanism is deliberated in section 3. The simulation and experimental measurements are presented in section 4. Further, section 5 presents the results for different cases and scenarios against reported SRPM protocol and finally, section 6 concludes the work.

6.2 RELATED WORK

Although scientists/researchers have proposed a number of routing protocols for different network environments, however, these protocols are basically espouse for homogenous systems and are designed keeping a non-trivial security in mind which are unable to perform well in heterogeneous mesh environments. Boushaba, Hafid and Gendreau have [143] proposed a gateway selection and source based routing mechanism to securely transfer the data packets to their intended destination nodes. The proposed mechanism selects the best routing path using a routing metric procedure which is basically a combination of certain networking parameters such as inter-flow, intra-flow interferences and packet loss ratio. Further the proposed protocol eliminates the issue of path changing phenomenon where the source node frequently switches to the new route in case of jitter and delays due to network congestion. The proposed mechanism eliminates this issue by computing a waiting time process where the source waits for some time before switching to the new routing path. The simulation results of proposed mechanism efficiently validate the network throughput, delay and packet loss ratio metrics over existing technique. Neumann et al. [110], have anticipated a secure decentralized routing mechanism for MANETs by ensuring the trust among concurrent and individual routing topologies. It enables a decentralized cryptographic negotiation technique among the communicating entities where the transmitted routing messages are encrypted using number of cryptographic signatures. The proposed protocol secured the routed packets against data plane attacks and control plane and validates the proposed phenomenon by analyzing the benchmark results over large number of nodes as compared to existing approach. Further, Talawar and Ramesh [111] have proposed an end-to-end secure communication through a trust based phenomenon by establishing a shared secret key between the neighbors. The generic assumption of all aforementioned routing mechanisms is that all the routers and gateways are cooperative and non-malicious during the packet
transmission. However to overcome the above discussed issues, Benitez et al. [144] projected a combination of elliptic curve digital signature and identity based encryption algorithm to secure the data packets in link state routing procedures. The elliptic curve digital signature ensures the confidentiality and integrity of routing messages while identity based encryption method prevents the routed messages from active and passive routing threats. The authors in [145-146] have proposed different schemes to quickly transfer the data packets by deriving time division multiple access (TDMA) schedule and Markov chain model is used in discrete time to enhance the performance of opportunistic routing protocols. Sbeiti and weitfeld [113] have provided a combination of digital signatures with symmetric block ciphers and lightweight authentication tree to ensure the security among routing messages. The lightweight authentication reduces the computational and communication overheads of routed messages while a symmetric block cipher eliminates the issue of key storage and key management overheads. Moreover, Khan et al. [114-115] have proposed a secure protocol for hierarchical mesh networks by modifying the basic Ad-hoc On-Demand Distance Vector routing mechanism; in this protocol the authors have designed a 2-hop information and passive acknowledgement mechanism to ensure the security against various routing attacks. However, it may increase the storage overhead at routers and instead of keeping the information of single-hop neighbor, routing table is storing the 2-hop information which may lead to extra overhead at routers. To exploit the characteristics of WMN, 802.11s standard is released by IEEE in which Hybrid Wireless Mesh Protocol (HWMP) is specified, but in this protocol security in forwarding and routing is not deliberated and is vulnerable to several routing attacks like the black hole, worm hole and falsification attacks [147-148]. A wormhole attack is the one where the malicious nodes forms a tunnel between the source and destination and re-route the data packets to some other nodes rather than forwarding to their intended destinations. Further, in black hole attack, the compromised or malicious node recommends itself as the shortest route to reach the end or destination node with the aim to drop the entire packet flow going towards it while falsification is the attack where an intruder hacks the legitimate node’s address with the aim of affecting the performance metrics of the network. These two attacks are taken as two severe routing attacks because they drastically affect the network performance.

Therefore, to prevent from these loopholes, an efficient secure routing mechanism is needed which can successfully transmit the data packets. From the recital point of view, the aforementioned secure routing protocols deal with flat network which are infeasible to
implement in hierarchical mesh environments and are vulnerable to a variety of routing attacks. In recent years, trust based methods have suit an active research domain as they have appeared as a viable solution to take the routing decision based on anticipated trust value of other nodes. Recently, we have reported [139] a weight trusted routing mechanism where the nodes having highest trust values would be considered during routing path formation. The trust value of each node is computed using SITO [149] and Dijkstra’s shortest path routing algorithm [150] is used to formulate the path among the nodes. The weight between each node is deliberated through certain parameters such as residual energy, packet loss ratio and the distance between each node. The node having highest trust value would have the lowest weight and would be considered during routing path formation.

In this work, we have implemented the WTR mechanism in smart home communication procedures for ensuring the security against routing attacks over static and dynamic nature of nodes (consisting of small or large number of nodes). The proposed mechanism is validated by highlighting the improvements in output results over certain parameters.

6.3 PROPOSED APPROACH

Figure 6.1 depicts the network model of the proposed mechanism consisting of n number of nodes among which some are assumed as malicious nodes m, where all the nodes are connected with each other by assigning some weights (as presented in Figure 6.1(b)). To securely transmit the message signals to their intended destination nodes, the shortest path Dijkstra’s routing algorithm is used where weights are assigned to each node by computing the TV of each node using certain parameters such as: 1) node distance which is calculated using Euclidian distance formula, in our proposed approach we have used Euclidian distance formula as it is used for various line of sight range applications like in sensors, which are placed in a room or in a hall to verify the range calculation. However, in case of obstacles like wall, the signals degrade by collision from the obstacles which affect the range of zigbee and hence routers are used for zigbee. 2) Node trust that is computed through social impact theory optimizer which states that trust of a node depends on the number of previous interactions of each node. In this, a social rank of each node is calculated using the parameters like residual energy and packets lost by the node in the network. Initially, each node is assigned some initial trust value ranging from 0.7- 0.95 with 1 as the highest trust value and then the trust value of a node is increased or decreased by checking its social rank using some predefined threshold value.
The formula for calculating the trust factor is given as:
\[ \text{Node Trust} = \sum_{i=1}^{n} \text{Previous interactions of node}, \]
where, “n” is the number of nodes, 3) residual energy which is left after transmission of data at each node and 4) packet loss ratio that is calculated at each node depending upon the overflow condition of packets (each node in a network consists of a fixed length queue and if the queue of a node is full then packets start dropping and it encounters overflow condition) and expiry TTL parameter (which is associated with each packet and decreases as the packet passes through a node).

So, the weight of each node is defined as the summation of the residual energy, packet loss ratio, distance between the nodes multiplied by some constant value and the negation of TV (the constant value is based on the weightage given to each parameter) as given in (1).

The negation of trust value is taken to satisfy the property of Dijkstra’s algorithm where the higher is the value of the trust, the lesser is the weight of each node that would be selected in routing path formation.

\[ w_n = \sum_{i=1}^{n} \left( \text{constvalue} \times \text{RE} + \text{constvalue} \times \text{PL} + \text{constvalue} \times D_{ij} \right) + (1 - TV) \quad (1) \]

The flowchart and the corresponding algorithm of the proposed mechanism are depicted in Figure 6.2 and Table 6.1 respectively. The proposed routing mechanism is based upon two key factors i.e. network metrics and security. The dynamic and broadcasting nature of mesh network not only increases the communication or scalability range of the network but also affects the performance metrics of the network during nodes’ mobility.
Further, the multi-hop feature invites a number of internal vulnerabilities where presence of any malicious behavior during routing path formation or packet transmission may affect the security and performance metrics of the network. The proposed approach relies on the design of Dijkstra’s routing algorithm and SITO optimizer.

The smart home architecture and its internal connectivity among the devices is depicted in Figure 6.1(a) and Figure 6.1(b) respectively. To clearly understand the proposed mechanism, let us take a scenario as illustrated in Figure 6.1(b) where source node ‘A’ wants to transmit some packets to the intended destination node ‘D’. Initially, let ‘S’, ‘U’ and ‘R’ be assumed as three adversary nodes affected by black hole attack which simply drop the entire packet flow coming towards them. After the transmission of some messages by these malicious nodes, their TV would be very less according to SITO (as they will drop the packet flow and increase the packet loss ratio along with an increase in residual energy) and their corresponding

![Flowchart of the proposed mechanism](image-url)
weights computed through the given formulas would be very high that they would never be considered during path formation process.

**Algorithm 1: Packet transmission mechanism of the proposed approach**

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Algorithm steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Initialize the process by assigning each node with a random trust value between 0.7-0.95</td>
</tr>
<tr>
<td>Step 2</td>
<td>For (i \leftarrow 0 : n; n) is the total number of nodes in the network</td>
</tr>
<tr>
<td>Step 3</td>
<td>For (j \leftarrow 0:n\ \forall j \neq i)</td>
</tr>
<tr>
<td>Step 4</td>
<td>(W_{ij} = \text{CalWeight}(S_i, S_j)), where S is the set of data required to calculate the weight for node i.</td>
</tr>
<tr>
<td>Step 5</td>
<td>End for</td>
</tr>
<tr>
<td>Step 6</td>
<td>End for</td>
</tr>
<tr>
<td>Step 7</td>
<td>(\text{FindRoute}(n_s, n_d)), Dijkstra’s algorithm for route discovery</td>
</tr>
<tr>
<td>Step 8</td>
<td>(\text{Transfer Data}(n_s, n_d))</td>
</tr>
<tr>
<td>Step 9</td>
<td>Go to step 2</td>
</tr>
</tbody>
</table>

As ‘\(S\)’ is a black hole affected node, so, the weight between ‘\(S - T\)’, ‘\(S - U\)’ and ‘\(S - D\)’ is very high i.e. 3, 3 and 4 (see Figure 6.1(b)) so they would never be considered during path formation process. Similarly, the weight computed between ‘\(U - D\)’ is 3 and is neglected during packet transmission process. The foremost advantage of the proposed approach is the process of computing a secure shortest routing path using Dijkstra’s algorithm among available number of routes. In an ideal case where all the nodes are trusted and cooperative with each other, the available number of routes to apply the Dijkstra’s algorithm between ‘\(S\)’ and ‘\(D\)’ would be \((i \times (i - 1))/2\) where ‘\(i\)’ is the number of intermediate nodes between the communicating entities while in case of malicious behavior, if the degree of malicious nodes is 2 (i.e. each node is linked with 2 edges) and the percentage of malevolent behavior is more than 30%, then the available number of paths would be reduced to \(1/3\) of ideal available routes else if the degree of malicious nodes is more than 2 (means the nodes have more than two connected edges) then the available paths would be more than 50%. The reason is that the nodes selected for path formation are based on their trust values; the node having lowest trust value would never be included for the path formation and would be excluded during route generation process. So, in a network size of 8 nodes where intermediate nodes are 6 between ‘\(S\)’ and ‘\(D\)’, and if nodes ‘\(R\)’ and ‘\(U\)’ are malicious (as presented in Figure 6.1(b)), then the total number of paths would be 5 (i.e. ‘\(A - P - T - D\)’, ‘\(A - Q - S - D\)’, ‘\(A - Q - T - D\)’, ‘\(A -

The possible availability of routes between ‘$S$’ and ‘$D$’ = \[
\left\{ \begin{array}{ll}
\frac{i \times (i-1)}{2}, & \text{during ideal case} \\
(i - 1) \text{and more than 50%}, & \text{during malicious behavior}
\end{array} \right.
\]

where ‘i’ is the total number of intermediate nodes available between S and D in a network size of ‘n’ nodes. Table 6.2 presents the algorithm to determine the number of routes available with the increment of malicious nodes in the network.

**Algorithm 2: The algorithm for computing the shortest path (using Dijkstra’s algorithm) among available number of nodes with the increment of malicious nodes.**

**Input:** Network size of ‘n’ nodes

**Output:** A single source shortest path is computed using Dijkstra’s algorithm from available possible paths

**Procedure:**

In a network size of ‘n’ nodes, the total number of intermediate nodes ‘i’ between source ‘$S$’ and destination ‘$D$’ would be n-2 i.e. i = (n-2)

// During Ideal case where number of nodes are cooperative with each other

The available number of routes among ‘$S$’ and ‘$D$’ would be $(i \times (i - 1))/2$

Among $(i \times (i - 1))/2$ available routes, a single source shortest path is calculated between communicating entities using Dijkstra’s routing algorithm

// During Attacker case where intermediate nodes among ‘$S$’ and ‘$D$’ are malicious ‘m’ in mature

If (percentage (%) of m $\geq 30\%$ and $m_{\text{degree}} == 2$)

Then

Available number of routes would be (i-1)

Else if (percentage (%) of m $\geq 30\%$ and $m_{\text{degree}} > 2$)

Then

Available number of routes would be more than 50%

End else if

End if
Therefore, the number of possible paths between the source node ‘A’ and destination node ‘D’ with their measured weights as depicted in Figure 6.1(b) are presented in the Table 6.1. According to Dijkstra’s algorithm, the shortest routing path used to forward the data packets would be through route-1 i.e. ‘A − P − T − D’, its nodes have the highest computed trust value and lowest assigned weights thus are more reliable and considered for secure message transmission.

6.4 NUMERICAL SIMULATION AND MEASUREMENTS

Table 6.1: The possible available routes between source ‘S’ and destination ‘D’.

<table>
<thead>
<tr>
<th>Routes</th>
<th>Paths</th>
<th>Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route 1</td>
<td>A-P-T-D</td>
<td>3</td>
</tr>
<tr>
<td>Route 2</td>
<td>A-Q-T-D</td>
<td>5</td>
</tr>
<tr>
<td>Route 3</td>
<td>A-Q-S-T-D</td>
<td>8</td>
</tr>
<tr>
<td>Route 4</td>
<td>A-Q-S-D</td>
<td>7</td>
</tr>
<tr>
<td>Route 5</td>
<td>A-R-U-D</td>
<td>7</td>
</tr>
<tr>
<td>Route 6</td>
<td>A-Q-U-D</td>
<td>7</td>
</tr>
<tr>
<td>Route 7</td>
<td>A-Q-S-U-D</td>
<td>7</td>
</tr>
<tr>
<td>Route 8</td>
<td>A-R-U-Q-S-D</td>
<td>11</td>
</tr>
<tr>
<td>Route 9</td>
<td>A-R-U-Q-T-D</td>
<td>9</td>
</tr>
<tr>
<td>Route 10</td>
<td>A-R-U-S-T-D</td>
<td>11</td>
</tr>
<tr>
<td>Route 11</td>
<td>A-R-U-S-D</td>
<td>11</td>
</tr>
<tr>
<td>Route 12</td>
<td>A-P-T-Q-S-D</td>
<td>9</td>
</tr>
<tr>
<td>Route 13</td>
<td>A-P-T-S-D</td>
<td>9</td>
</tr>
<tr>
<td>Route 14</td>
<td>A-P-T-Q-U-D</td>
<td>9</td>
</tr>
<tr>
<td>Route 15</td>
<td>A-P-T-S-U-D</td>
<td>11</td>
</tr>
</tbody>
</table>

The performance efficiency of WTR mechanism against reported SRPM protocol has been first investigated through simulations using NS2 and afterwards is tweaked to map the real performance using experimental outcomes. The SRPM protocol is taken as the base paper of this chapter as it ensures the security without using any cryptographic technique in hierarchical mesh networks.
6.4.1 Simulation setup
The simulation is based upon IEEE 802.11 standard in an area of 400m×400m, where the nodes are randomly distributed to execute the reported SRPM as the basic approach and WTR as the proposed protocol. In a network area of 400m×400m, constant bit rate traffic type is taken having 512 bytes of packet size where the nodes are mobile and assumed to be selfish in nature. The simulation time that we have considered is 70 seconds, it can be extended to any length as the packet generation is 512 bytes per second. The simulation time that we have used is a considerable amount of time to depict the behavior of proposed topology. The selfish nodes may drop, duplicate and selectively forward the data packets by indulging into some unethical activities (i.e. packet/route modification, non-optimal route selection etc.). Table 6.2 illustrates the entire information regarding the simulation setup.

Table 6.2: The simulation parameters for the proposed mechanism.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Nodes</td>
<td>(10-25), (100-900)</td>
</tr>
<tr>
<td>Grid Dimension</td>
<td>400 m × 400 m</td>
</tr>
<tr>
<td>Routing protocol</td>
<td>AODV</td>
</tr>
<tr>
<td>Propagation Model</td>
<td>Two-ray ground</td>
</tr>
<tr>
<td>Radio Range</td>
<td>120m</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>MAC Protocol</td>
<td>MAC 802.11</td>
</tr>
<tr>
<td>Link Bandwidth</td>
<td>2 mbps</td>
</tr>
<tr>
<td>Mobility Rate</td>
<td>0-25 m/s</td>
</tr>
<tr>
<td>PHY Layer</td>
<td>PHY 802.11</td>
</tr>
<tr>
<td>Antenna</td>
<td>Omni antenna</td>
</tr>
<tr>
<td>Simulation Period</td>
<td>70 sec</td>
</tr>
<tr>
<td>Protocols</td>
<td>WTR (proposed), SRPM (basic)</td>
</tr>
</tbody>
</table>

6.4.2 Experimental Setup
For the practical implementation, Zigbee wireless technology is used consisting of 8 mesh nodes to form a network. In the Zigbee network, three types of nodes can be formed, first is gateway which acts as a hub and provides the services to the end nodes, second one are routers whose task is to perform the message generation and message forwarding operations and third are the end nodes which can generate the data without forwarding capabilities. The type of data depends on the applications of the node. The embedded hardware used is a Roboard RB-110 with a vertex X86 32 bit CPU running at 1200 MHZ and 256 DRAM.
Further, the software which controls and forwards the data in Zigbee network is XCTU. The experimental results are extracted from XCTU.

6.5 RESULTS AND DISCUSSION

In this section, the reported SRPM and the proposed WTR protocol are simulated through network metrics under three different cases as discussed in section Introduction. We have considered several network sizes in fixed as well as in dynamic environments for ideal and adversary models to identify the novelty of the proposed mechanism. This section is divided into three different cases to compute the metrics of both the approaches in scalable network sizes. The first two cases show the metrics results computed through NS2 simulator over 25 and 900 number of nodes in fixed and dynamic environments while the remaining case presents the validity of the proposed mechanism by considering two routing attacks in two different scenarios.

Case 1: Network metrics are measured against small (10-25) and large (100-900) number of nodes over fixed network sizes.

The depicted Figure 6.3(a) presents end-to-end delay of both the approaches over increasing number of nodes which is increasing linearly with a delay difference of 80 milliseconds which means that the proposed approach is 80msec faster than the basic approach up to 25 number of nodes.

In a network size of 10 nodes, the delay of the proposed approach is 235 milliseconds and that of the basic approach is 300 milliseconds, therefore, the delay difference of basic and the proposed approach is (300-235) i.e. 65 msec. Similarly, in a network size of 15 nodes, the delay difference is 80 millisecond, therefore, the average delay difference up to 25 number of nodes between basic and the proposed approach is 80 msec (approximately) which is maintained through all the network sizes. Figure 6.3(b) shows the % of message delivery ratio (MDR) over increasing network sizes. The MDR % of both the approaches is decreasing linearly with a difference of 2.50% and is maintained up to network sizes of 25 nodes. The throughput % of the proposed approach outperforms basic approach with a difference of huge % as depicted in Figure 6.3(c). The throughput computed using basic approach (in %) is decreasing with increasing values of the network size while in the proposed approach, it is decreasing up to lower values of the network size and after network size of 15 nodes, it is decreasing at a lower rate as compared to the network size of smaller values.
Figure 6.3(d), Figure 6.3(e) and Figure 6.3(f) present the end-to-end delay, MDR and throughput % for large network sizes respectively. As depicted from the figures, the metrics of the proposed approach are increasing at a constant value after a network size of 600 nodes while the delay and % of MDR and throughput of the basic approach are increasing and decreasing significantly.
The network metrics of both basic and the proposed protocol against scalable network sizes (a) end-to-end delay over small network size (b) MDR % over small network size (c) throughput % over small network size (d) end-to-end delay over large network size (e) MDR % over large network size (f) throughput % over large network size

The proposed approach performs better against basic approach because the proposed mechanism uses Dijkstra’s algorithm which has the advantage that it considers the positive weights for path formation and never chose the same path again, however in the case of basic approach, the network metrics are continuously increasing or decreasing up to 900 numbers of nodes because it considers the negative weights and same path again and again for packet transmission which delays the path formation process and affects the metrics in the network.

**Case 2: Network metrics under scalable network sizes in dynamic nature where node are mobile and moving at the speed of 0-25 m/s**

The depicted Figure 6.4(a)-(f) shows the network metrics in dynamic nature where the number of nodes are dynamic in % over all network sizes.

The dynamic environment is changing due to node placement and communication pattern including the packet generation mechanism in mobile topology which every time affects the certain network metrics such as packet delivery ratio and delay of the network. Figure 6.4(a), Figure 6.4(b) and Figure 6.4(c) show the end-to-end delay, % of MDR and throughput over increasing % of mobile nodes respectively. The delay and % of MDR and throughput is increasing and decreasing at a constant rate over small network sizes while the values are almost constant for both basic and the proposed approach in large network sizes. The delay difference and % difference of MDR and throughput of the proposed and basic approach are 594 milliseconds, 7.2% and 6.4% respectively which outperforms the basic approach.

**Case 3: Network metrics are measured against black hole and falsification attacks over scalable network sizes**

In this case, the performance of the proposed protocol is measured over various adversary nodes by considering two different scenarios. Scenario-1 presents the metrics results by varying the number of black hole and falsification routing attacks while the validity of the proposed mechanism is scrutinized by increasing the number of black hole and falsification nodes near source and destination over small and large network sizes.
Figure 6.4 Network metrics of basic and the proposed protocol under dynamic nature (a) end-to-end delay over small network size (b) MDR % over small network size (c) throughput % over small network size (d) end-to-end delay over large network size (e) MDR % over large network size (f) throughput % over large network size.
Figure 6.5 Network metrics by increasing the percentage of black hole and falsify attacks over small and large network sizes (a) end-to-end delay over small network size (b) MDR % over small network size (c) throughput % over small network size (d) end-to-end delay over
large network size (e) MDR % over large network size (f) throughput % over large network size.

**Scenario-1: Black hole and Falsification attacks are increasing at different percentage.**

To validate the proposed mechanism, numbers of nodes are increasing at the percentage of 10, 20, 50 and 70 over small and large network sizes under fixed environment. Figure 6.5 (a)-(f) shows the end-to-end delay, MDR % and throughput percentage during black hole attack. By increasing the number of black hole nodes, the proposed approach performs better as compared to the basic approach. The end-to-end delay of black hole and falsification attacks over small network sizes is increasing significantly as depicted in Figure 6.5(a) and Figure 6.5(g) while the MDR and throughput (%) is increasing linearly in both the attacks over small network sizes as depicted in Figure 6.5(b), Figure 6.5(c), Figure 6.5(h) and Figure 6.5(i). In large network sizes, the metrics results are constant after 50% of mobile nodes in the proposed approach while the values are increasing continuously in basic approach. The good metrics results of the proposed mechanism over basic approach are because the packets are transmitted to only the nodes which are trusted and can securely transfer the packets to their destination nodes but as the number of black hole nodes increase, the basic approach results reduce drastically because firstly it considers negative weights and enters into infinite route formation and secondly the packets are transmitted without any trust value which enhances the chances of performance degradation. Further, Figure 6.5(g)-(l) show the results during falsification attack, the chances of falsification attacks during the proposed approach reduce due to their trust values while the basic approach may overcome the attacks through passive acknowledgement and 2-hop information but may increase the time of path formation and packet transmission process. Therefore, the values of the proposed approach are almost flat in large networks. By increasing the % of black hole and falsification attacks, in both fixed and dynamic scenarios, the path recovery and packet transmission timings of basic approach increase because firstly it identifies the attacker through passive acknowledgement process and secondly it applies the recovery process using 2-hop information while the proposed approach never allows the malicious nodes to enter during path formation process.

**Scenario-2: Increasing black hole and falsification nodes near source and sink nodes over small and large network sizes.**
Figure 6.6 Network metrics by increasing the number of black hole and falsify nodes near the source and sink nodes (a) end-to-end delay over small network size (b) MDR % over small network size (c) throughput % over small network size (d) end-to-end delay over large network size (e) MDR % over large network size (f) throughput % over large network size
To deeply understand the proposed phenomenon, the metrics are measured against both the attacks by increasing them near the source and sink nodes. The depicted Figure 6.6(a)-(f) shows the outcomes of network metrics by increasing the adversary nodes near source and sink nodes.

![Graph showing network metrics](image)

**Figure 6.7** Experimental results over increasing number of nodes (a) End-to-End Delay (b) MDR %.

As the numbers of black hole nodes are increasing near the source and sink nodes, the end-to-end delay is increasing but MDR% and percentage of throughput are affected at a constant rate in the proposed mechanism. To validate the approaches, Figure 6.7(a) and Figure 6.7(b) show the experimental results of the proposed and basic approach against end-to-end delay and MDR percentage. The experimental values are same as the values simulated through NS2 simulator. In a network size of 8 nodes, the experimental end-to-end delay of the proposed approach is 186 milliseconds while through NS2 simulator the delay is 190 approximately which is same as experimental result. Similarly, the MDR % of the proposed mechanism is 97.53% through experimental and 97.50% using NS2 simulator. The proposed mechanism significantly reduces the delay because of its fastest path formation process and packet transmission through trust factors. Further, the MDR% of the proposed mechanism also shows better results because of its positive weight computation through SITO optimizer.

### 6.6 SECURE HANDOFF ROUTING IMPLEMENTATION IN SMART HOME ENVIRONMENTS

The secure routing mechanism is extended over handoff procedures where mesh clients or devices are mobile in nature.
Figure 6.8 Packet delivery ratio

Figure 6.9 Network throughput

Figure 6.10 Packet loss rate (during black hole)
Figure 6.11 Packet loss rate (during wormhole)

During the mobility, the security is checked after authenticating the mesh clients or devices and securely routing their data transmission against a number of routing layer threats. Black hole and data falsification attacks are considered to analyze the proposed mechanism because of their severe malicious characteristics. The proposed mechanism is simulated over NS2 simulator against previously proposed handoff and routing mechanisms by measuring their certain network metrics as depicted in Figure 6.8, 6.9, 6.10 and 6.11 against packet drop ratio, network and packet loss ratio over black hole and wormhole attack.

6.7 CONCLUSION AND FUTURE WORK

In this chapter, the WTR mechanism using SITO optimizer has been exploited to perceive and eliminate the malevolent nodes concerned during the routing path formation and implemented for smart home communication procedures that are based on hierarchical mesh networks. The proposed mechanism has significantly reduced the end-to-end delay and increased the message delivery ratio and throughput percentage in presence of black hole and falsification attacks over small and large network sizes under fixed and dynamic environments. The simulation using NS2 simulator validates the proposed mechanism up to 900 numbers of nodes and illustrates that the proposed mechanism reaches up to a constant level of values against end-to-end delay, message delivery ratio and throughput percentage in comparison of the reported SRPM protocol. In addition to this, we have validated the proposed approach with experimental results at smaller values of the network sizes. However, the energy
consumption in the large network sizes during the packet transmission/reception is a potential issue which will be detailed in future communication.