Wireless Pers Commun (2018) 98:2367–2387
https://doi.org/10.1007/s11277-017-4978-5

Aspects of Trusted Routing Communication in Smart Networks

Geetanjali Rathee[1] · Hemraj Saini[1] · Ghanshyam Singh[2]

Published online: 6 October 2017

Abstract In this paper, we have exploited the weight trusted routing (WTR) mechanism to detect and eliminate the malicious nodes involved during the routing path formation in smart-home environments where the routing between the communicating entities is performed through the mesh architecture. Further, 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 and trust value of each node which is computed using social impact theory optimizer. Moreover, we have presented 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 commercial simulator NS2 is used to simulate and compare the network metrics for both conventional as well as proposed approach and is validated with experimental results over end-to-end delay and message delivery ratio against reported literature.

Keywords Wireless mesh network · Social impact theory optimizer · Weight trusted routing · Falsification attack · Black-hole attack · Scalability · Smart home security

✉ Ghanshyam Singh
ghanshyam.singh@juit.ac.in

Geetanjali Rathee
geetanjali@juit.ac.in

Hemraj Saini
hemraj.saini@juit.ac.in

[1] Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat, Solan 173 234, India

[2] Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Waknaghat, Solan 173 234, India

1 Introduction

With the recent societal development, the demand of digital environments where an individual can interacts smartly with its surroundings to increase comfort zone as compared to the hard build infrastructures, is gradually accumulating. The smart cities, smart homes and smart societies are potentially hot trends of intelligent environments where multiple internet-of-things (IoT) devices respond like human behavior by automatically controlling and adapting the environmental circumstances [1, 2]. In order to provide the interconnectivity among 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 [3, 4]. Currently, the Zigbee is one of the most widely used wireless technology for such systems because of its mesh based architecture which allows high scalability and provides large coverage area by incorporating self-healing, self-organizing and self-configuring characteristics [5, 6]. Although, the main purpose 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 such environments is a challenging task particularly, 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 over the security is the nature of fundamental routing protocols [7–9] 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 networks. 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 purpose rather than being collectively or maliciously disclosed for the function of violating their autonomy and privacy [10, 11].

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 where the attackers may launch several types of attacks either by compromising the legitimate routing nodes or by disrupting the data packets [12–14]. Therefore, one standard approaches to counter such attacks is secure routing. Various proposed approaches use cryptographic techniques to ensure the integrity and confidentiality of the nodes using trusted third party [15–17]. However, this technique seems to be infeasible in mesh environments due to certain parametric issues such as computational complexity, communication overhead, storage issues as well as its broadcasting and dynamic nature. Further, cryptographic technique is effective for external attacks and is found completely infeasible to ensure the security against internal threats. 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 conquer the aforementioned issues. A number of trust based methods have been proposed for mobile ad hoc networks (MANETs) [18], wireless sensor networks (WSNs) [19, 20] and other networks [21, 22] which are basically espouse for homogenous systems and cannot be adapted well in heterogeneous mesh networks because of their multi-hop and dynamic nature [23, 24]. Therefore, there is a potential demand to provide a secure communication mechanism that overcomes the computational complexity, communication overhead, storage issues and ensures efficient routing procedures to establish the communication in mesh based smart home environments. In the next section, we have overviewed recent related work and formulate the research problem.

2 Related Work

Recently, various scientists/researchers have proposed a number of routing protocols [25–27] for different network environments. However, these protocols are basically espouse for homogenous systems and are designed considering a non-trivial security therefore unable to perform well in the heterogeneous mesh environments. Boushaba et al. [28] have 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 combination of certain networking parameters such as inter-flow as well as 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 new route in case of jitter and delays due to network congestion. Moreover, 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. [29] 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 secures the routed packets against data plane and control plane attacks and the proposed phenomenon is validated by analyzing the benchmark results over large number of nodes as compared to existing approach. Further, Talawar and Ramesh [30] 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 discussed issues, Benitez et al. [31] have 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 the identity based encryption method prevents the routed messages from active and passive routing threats. The authors in [32, 33] 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 [34] have provided a combination of digital signatures with symmetric block ciphers and light weight authentication tree to ensure the security among routing messages. The light-weight 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. To exploit the characteristics of wireless mesh network (WMN), 802.11 s standard is released by IEEE in which the hybrid wireless mesh protocol (HWMP) is specified. However, in this protocol security in routing procedures is not deliberated and is vulnerable to several routing attacks like the black hole, worm hole and falsification [35, 36]. In the worm hole attack, 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. In the black hole attack, the compromised or malicious node offers itself as the shortest route to reach the destination so that it can drop the entire packet flow departing towards it. However, the falsification is attack where an intruder hacks the legitimate node's address with the aim of affecting the performance metrics of network. These attacks are taken as severe routing attacks because they drastically affect the network performance. Moreover, Khan et al. [37, 38] 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 two-hop information and passive acknowledgment 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 two-hop information which may lead to extra overhead at routers.

With the performance 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, the 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 [39] a weight trusted routing mechanism where the nodes having highest trust value are considered during the routing path formation. The trust value of each node is computed using social impact theory optimizer (SITO) [40], and Dijkstra's shortest path routing algorithm [41] is used to formulate the routing path among the nodes. The weight between each node is deliberated through certain parameters such as residual energy, packet loss ratio and distance between each node. The node having highest trust value has the lowest weight and has been considered during routing path formation. Further, the Dijkstra's algorithm is chosen because of its small computational complexity as compared to that of the other short path routing algorithms such as Bellman–Ford algorithm used by [37, 38] to explore secure approach. Further, it considers positive weights to avoid the loop formation process. However, the greedy algorithms like greedy parameter circuit routing (GPCR) algorithm is unable to provide the accurate measurements and need to test on similar environments where its results should be comparable with the existing approaches repeatedly.

In this paper, 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. 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) and is validated by highlighting the improvements in output results over certain parameters. The author's potential contribution for the secure routing mechanism is summarized as follows.

- The Dijkstra's shortest path routing algorithm is employed to yield the shortest path between the communicating entities whose weights are assigned according to their trust factor that is computed using certain factors such as 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-time environment to analyze and evaluate the network metrics against proposed and reported secure routing protocol mechanism (SRPM) which is considered as the basic approach as reported in [37, 38].
- The behavior of both the protocols (proposed and basic) is initially analyzed under small network sizes and then explored over large network sizes having fixed number of nodes against different network metrics. Further, the network metrics are measured over scalable network sizes with mobile nature where the nodes are moving with speed of 0–25 m/s.

- The proposed protocol is validated under various adversary nodes having two different scenarios: (1) when the metrics are measured against two severe routing attacks i.e. black hole and falsification over the scalable network sizes, and (2) the performance is checked by increasing the number of black hole and falsification nodes near source and destination over small and large network sizes.
- Moreover, the experimental results are presented for end-to-end delay and message delivery ratio (%) for both the approaches.

The remainder of the paper is organized as follows. The proposed WTR mechanism is deliberated in Sect. 3. The simulation and experimental measurement results are presented in Sect. 4. Further, Sect. 5 presents the results for different cases and scenarios against proposed and reported SRPM protocol and finally, Sect. 6 concludes the work.

3 Proposed Approach

Figure 1 depicts the network model of the proposed mechanism consisting of n number of nodes among which m nodes are assumed as malicious where all the nodes are connected with each other by assigning weights (as presented in Fig. 1b). For secure transmission of the message signals to intended destination nodes, the shortest path Dijkstra's routing algorithm is used where the weights are assigned to each node by computing the trust value (TV) of each node using certain parameters such as:

1. Node distance which is computed using Euclidian distance formula. In the proposed approach, we have used Euclidian distance formula as it is utilized for various line-of-sight range applications like sensor nodes, which are placed in a room or in a hall to verify the range computation [41]. However, in case of obstacles like wall, the signals degrade by collision with the obstacles which affects the range of Zigbee and hence routers are used.
2. Node trust that is computed through SITO which states that the trust of a node depends on the number of previous interactions of each node. In this, the social rank of each node is calculated using the parameters like residual energy and packets lost by the node in network. Initially, each node is assigned some initial trust value ranging from 0.7 to 0.95 with 1 as the highest trust value and then the trust value of a node is

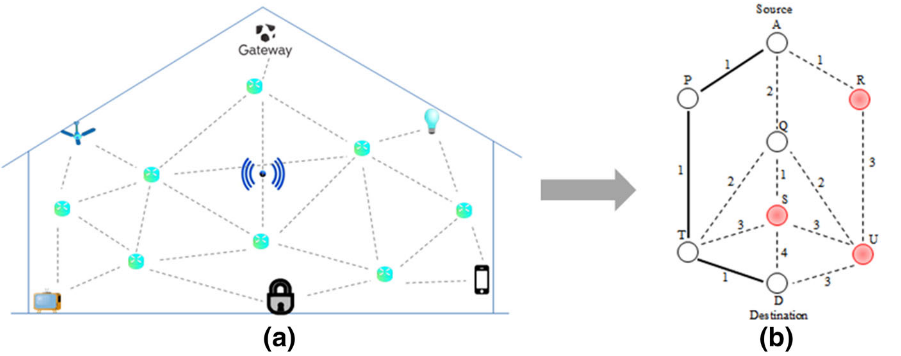

Fig. 1 The network model of proposed mechanism. **a** Mesh network in smart homes, **b** path formation among available number of routes through trust value

increased or decreased by checking its social rank using predefined threshold value. The formula for calculating the trust factor is given as:

$$\text{Node Trust} = \sum_{i=1}^{n} \text{Previous interactions of node,}$$

3. Residual energy which is left after transmission of data at each node.
4. Packet loss ratio which 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
5. Expiry time-to-live (TTL) parameter which is associated with each packet and decreases as the packet passes through a node.

Thus, the weight of each node is defined as the summation of the residual energy (RE), packet loss ratio (PL), distance between the nodes ($D_{i,j}$) multiplied by some constant value and the negation of TV (the constant value is based on the weightage given to each parameter) as in (1).

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

$$\mathrm{w_n} = \sum_{i=1}^{n} \left(\text{const value} \times \mathrm{RE} + \text{const value} \times \mathrm{PL} + \text{const value} \times \mathrm{D_{i,j}}\right) + (1 - \mathrm{TV}) \quad (1)$$

The flowchart and the corresponding algorithm of the proposed mechanism are depicted in Fig. 2 and Algorithm 1, respectively. The proposed routing mechanism is based on 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 node's mobility. Further, the multi-hop feature invites a number of internal vulnerabilities where the 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.

The smart home architecture and its internal connectivity among the devices is depicted in Fig. 1a, b, respectively. To clearly understand the proposed mechanism, let us consider a scenario as illustrated in Fig. 1b where the source node '*A*' wants to transmit data/information packets to the intended destination node '*D*'. Initially, let '*S*', '*U*' and '*R*' are 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 is 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 weights computed through (1) are very high which are never considered during the path formation process.

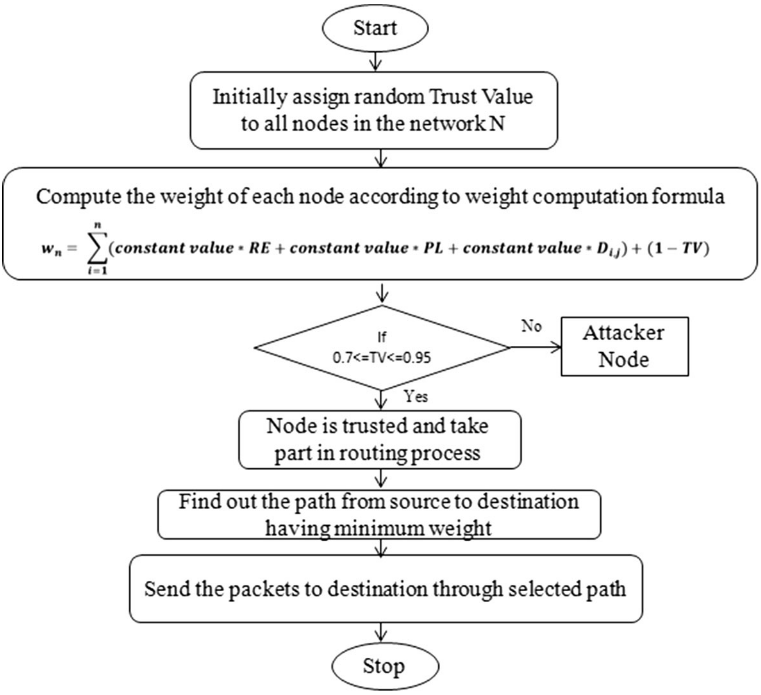
Start
Initially assign random Trust Value to all nodes in the network N
Compute the weight of each node according to weight computation formula
$w_n = \sum_{i=1}^{n}(constant\ value * RE + constant\ value * PL + constant\ value * D_{i,j}) + (1 - TV)$
If 0.7<=TV<=0.95
No
Attacker Node
Yes
Node is trusted and take part in routing process
Find out the path from source to destination having minimum weight
Send the packets to destination through selected path
Stop

Fig. 2 Flowchart of the proposed mechanism

Algorithm 1: Packet transmission mechanism of the proposed approach

```
S. No.   Algorithm steps
Step 1   Initialize the process by assigning each node with a random trust value between 0.7-0.95
Step 2   For i ← 0 :n; n is the total number of nodes in the network
Step 3     For j ← 0:n  ∀ j ≠ i
Step 4       $W_{ij} = \mathrm{CalWeight}(S_i, S_j)$, where S is the set of data required to calculate the weight for node i.
Step 5     End for
Step 6   End for
Step 7   FindRoute($n_s$ , $n_d$), dijkstra's algorithm for route discovery
Step 8   Transfer Data($n_s$, $n_d$)
Step 9   Go to step 2
```

As '*S*' is a black hole affected node, therefore the weight between '*S–T*', '*S–U*' and '*S–D*' is very high i.e. 3, 3 and 4 (Fig. 1b) therefore, they are never considered during path formation process. Similarly, the weight computed between '*U–D*' is 3 and is neglected during the 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 cooperate 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. However, 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 are 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 are 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 is never included for the path formation and excluded during the route generation process. Therefore, in a network size of 8 nodes where the intermediate nodes are 6 between ‘*S*’ and ‘*D*’, and if nodes ‘*R*’ and ‘*U*’ are malicious (as presented in Fig. 1b), then the total number of paths is 5 (i.e. ‘*A–P–T–D*’, ‘*A–Q–S–D*’, ‘*A–Q–T–D*’, ‘*A–Q–S–T–D*’, ‘*A–Q–T–S–D*’) while if ‘P’ and ‘R’ are malicious nodes then paths are 50% of ideal case (i.e. ‘*A–Q–S–D*’, ‘*A–Q–T–D*’, ‘*A–Q–U–D*’, ‘*A–Q–S–T–D*’, ‘*A–Q–U–S–D*’, ‘*A–Q–T–S–D*’, ‘*A–Q–T–S–U–D*’ and ‘*A–Q–U–S–T–D*’).

The possible availability of routes between ‘*S*’ and ‘*D*’ $= \left\{ \begin{array}{ll} \dfrac{i \times (i-1)}{2}, & duirng\ ideal\ case \\ (i-1)\ and\ more\ than\ 50\%, & during\ malicious\ behavior \end{array} \right\}$, where ‘*i*’ is the total number of intermediate nodes available between S and D in a network size of ‘*n*’ nodes. The Algorithm 2 determines 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:
Step 1      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 */
Step 2      The available number of routes among ‘S’ and ‘D’ would be $(i * (i-1))/2$
            Among $(i * (i-1))/2$ 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 */
Step 3      If (percentage (%) of m >=30% and $m_{degree}$ ==2)
            Then
               Available number of routes would be (i-1)
Step 4      Else if (% of m >=30% and $m_{degree}$>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 Fig. 1b are presented in the Table 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.

Table 1 The available routes between source '*S*' and destination '*D*'

Routes	Paths	Weights
Route 1	A–P–T–D	3
Route 2	A–Q–T–D	5
Route 3	A–Q–S–T–D	8
Route 4	A–Q–S–D	7
Route 5	A–R–U–D	7
Route 6	A–Q–U–D	7
Route 7	A–Q–S–U–D	7
Route 8	A–R–U–Q–S–D	11
Route 9	A–R–U–Q–T–D	9
Route 10	A–R–U–S–T–D	11
Route 11	A–R–U–S–D	11
Route 12	A–P–T–Q–S–D	9
Route 13	A–P–T–S–D	9
Route 14	A–P–T–Q–U–D	9
Route 15	A–P–T–S–U–D	11

4 Numerical Simulation and Measurements

The performance efficiency of WTR mechanism against reported SRPM protocol has been investigated through simulations using NS2 and afterwards is tweaked to map the real time performance using experimental outcomes. The SRPM protocol is chosen as the base paper as it ensures the security without using any cryptographic technique in hierarchical mesh networks.

4.1 Simulation Setup

The simulation is based upon IEEE 802.11 standard in the area 400 m × 400 m, 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 400 m × 400 m, constant bit rate traffic type is chosen with 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 s, 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 2 illustrates the entire information regarding the simulation setup.

4.2 Experimental Setup

For practical implementation, the Zigbee wireless technology employed consist of 8 mesh nodes to form a network. In the Zigbee network, three types of nodes are formed: (1) gateway which acts as a hub and provides the services to the end nodes, (2) routers whose task is to perform the message generation and message forwarding operations and (3) 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-

Table 2 The simulation parameters for proposed mechanism

Parameters	Values
Number of nodes	(10–25), (100–900)
Grid dimension	400 m × 400 m
Routing protocol	AODV
Propagation model	Two-ray ground
Radio range	120 m
Packet size	512 bytes
MAC protocol	MAC 802.11
Link bandwidth	2 mbps
Mobility rate	0–25 m/s
PHY layer	PHY 802.11
Antenna	Omni antenna
Simulation period	70 s
Protocols	WTR (proposed), SRPM (basic)

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.

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 Sect. 1. 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. In this section, we have considered three different cases to compute the metrics of both the approaches in scalable network sizes. The first two cases show the metric 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 Fig. 3a presents end-to-end delay of both the approaches over increasing number of nodes that are increasing linearly with a delay difference of 80 ms which means that the proposed approach is 80 ms faster than the basic approach up to 25 number of nodes.

In a network size of 10 nodes, the delay of proposed approach is 235 ms and that of the basic approach is 300 ms, therefore, the delay difference of basic and proposed approach is (300–235) i.e. 65 ms. Similarly, in a network size of 15 nodes, the delay difference is 80 ms, therefore, the average delay difference up to 25 number of nodes between basic and the proposed approach is 80 ms (approximately) which is maintained through all the network sizes. Figure 3b shows the percentage message delivery ratio (MDR) over increasing network sizes. The percentage MDR of both the approaches is decreasing linearly with a difference of 2.50 percent and is maintained up to network size of 25 nodes.

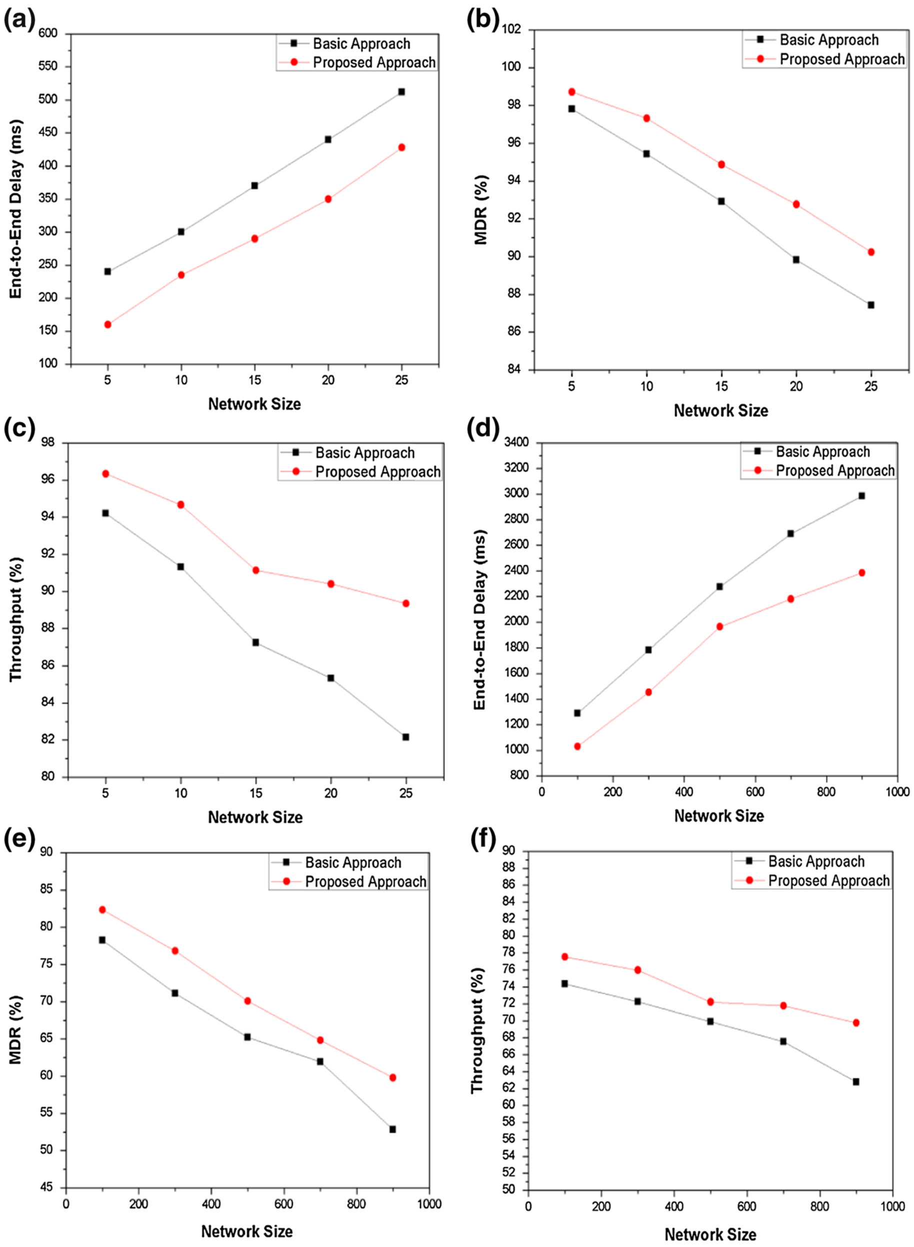

Fig. 3 The network metrics of both basic and the proposed protocol against scalable network sizes. **a** End-to-end delay over small network size, **b** MDR % over small network size, **c** throughput % over small network size, **d** end-to-end delay over large network size, **e** MDR % over large network size, **f** throughput % over large network size

The throughput percentage of the proposed approach outperforms basic approach with a difference of huge % as depicted in Fig. 3c. 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 3d–f present the end-to-end delay, MDR and throughput % for large network sizes, respectively. As depicted in the figures, the metrics of proposed approach are increasing at a constant value after a network size of 600 nodes while the delay and percentage of MDR and throughput of the basic approach are increasing and decreasing significantly. The reason of outperforming results of the proposed mechanism on both network sizes is the Dijkstra's approach which never considers the path again once it is chosen and considers positive weight for the path formation, however in the case of basic approach, the network metrics are continuously increasing or decreasing up to 900 numbers of nodes, also because the basic approach considers the negative weights and same path again and again for packet transmission, it delays the path formation process and affects the metrics in 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 Fig. 4a–f shows the network metrics in dynamic nature where the number of nodes are dynamic in percentage 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 certain network metrics such as packet delivery ratio and delay of the network. Figure 4a–c shows the end-to-end delay, percentage of MDR and throughput over increasing percentage of mobile nodes, respectively. The delay and percentage of MDR and throughput increases and decreases with a constant rate over the small network sizes while the values are almost constant for both the basic and proposed approach in large network sizes. The delay difference, percentage difference of MDR and throughput of the proposed and basic approach are 594 ms, 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 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 the source and destination over small and large network sizes.

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 5a–f shows the end-to-end delay, percentage MDR and throughput percentage during the black hole attack. By increasing the number of black hole nodes, the proposed approach performs better as compared to that of the basic approach. The end-to-end delay of black hole and falsification attacks over small network sizes is increasing significantly as depicted in Fig. 5a, g while the MDR and throughput (%) are increasing linearly in both

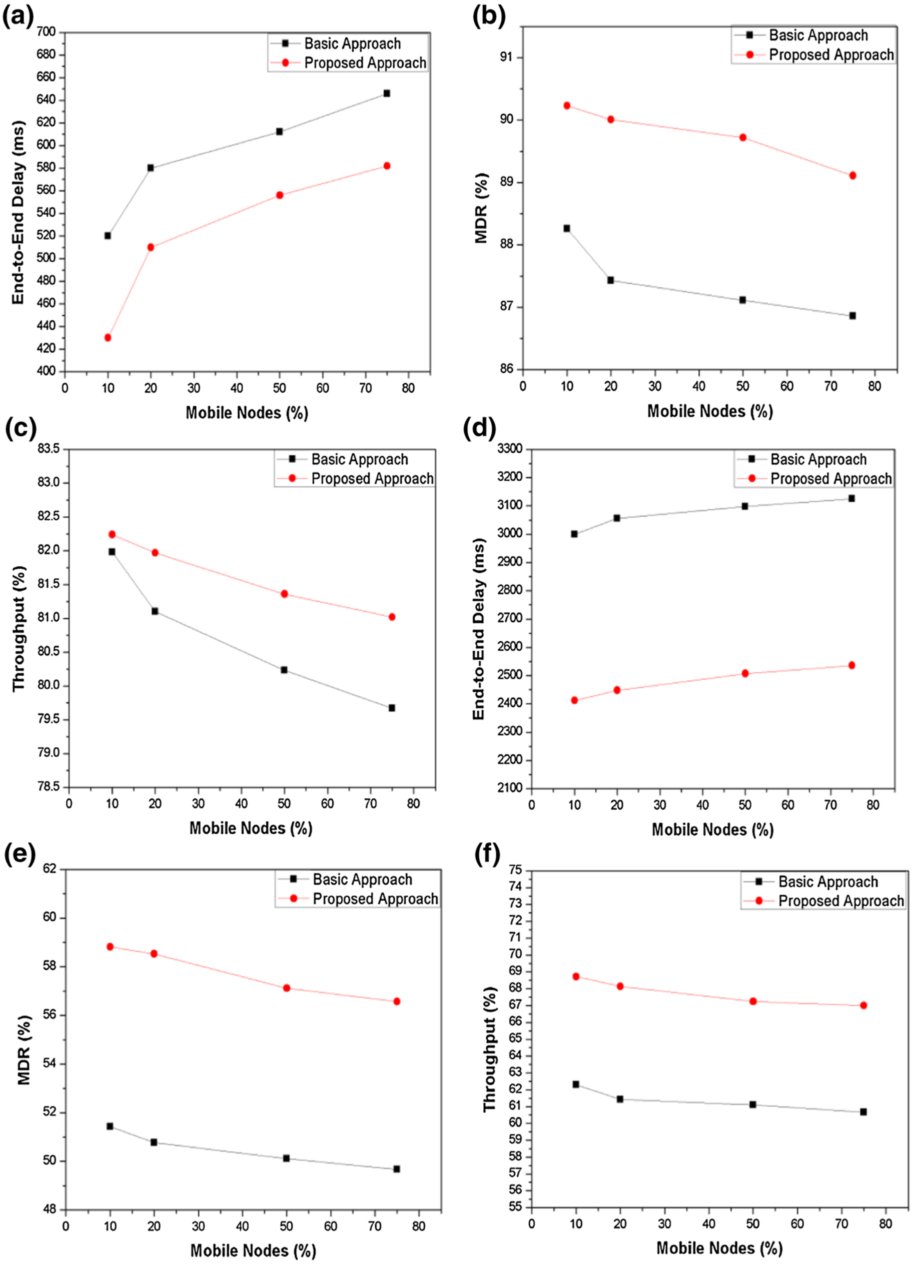

Fig. 4 Network metrics of basic and the proposed protocol under dynamic nature. **a** End-to-end delay over small network size, **b** MDR % over small network size, **c** throughput % over small network size, **d** end-to-end delay over large network size, **e** MDR % over large network size, **f** throughput % over large network size

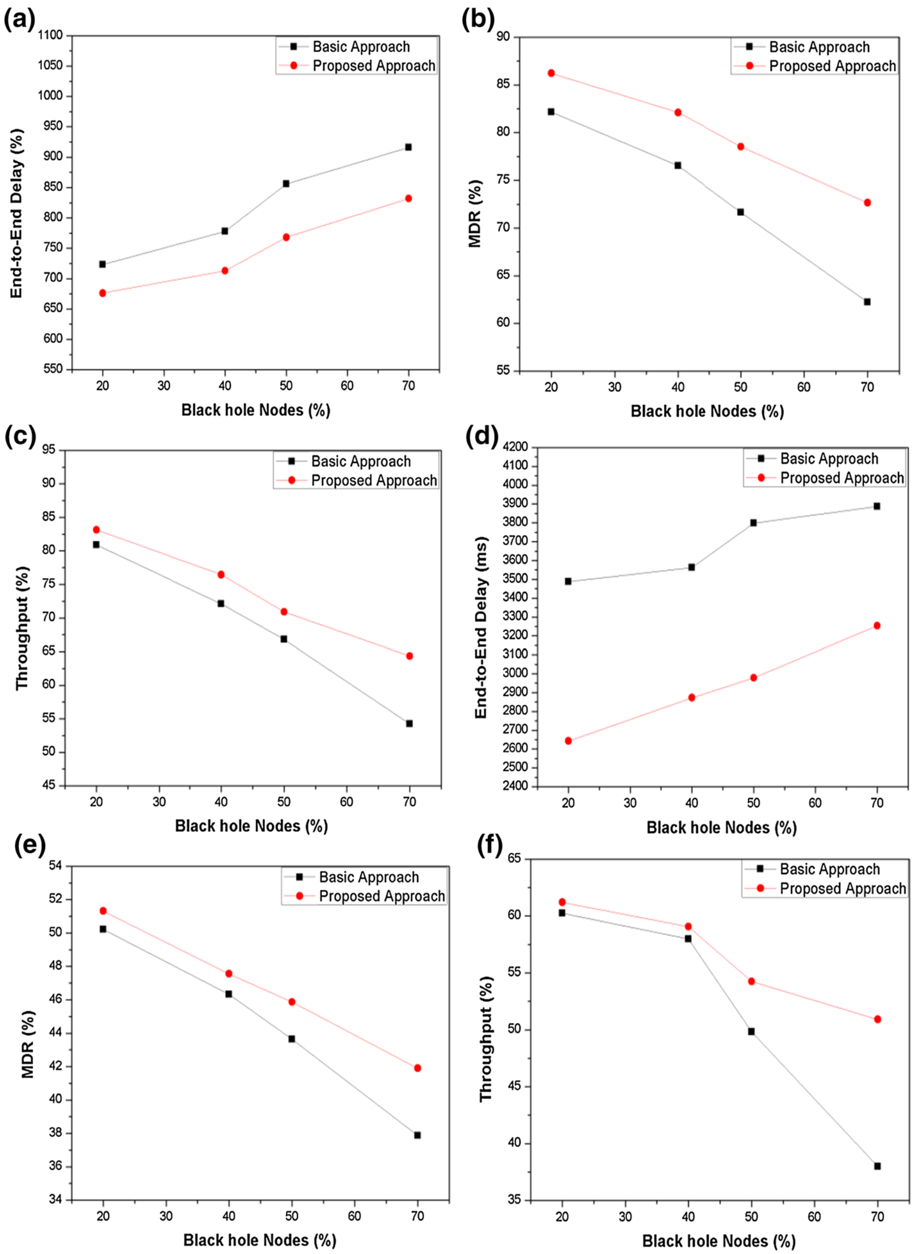

Fig. 5 Network metrics by increasing the percentage of black hole and falsify attacks over small and large network sizes. **a** End-to-end delay over small network size, **b** MDR % over small network size, **c** throughput % over small network size, **d** end-to-end delay over large network size, **e** MDR % over large network size, **f** throughput % over large network size **g** End-to-end delay during falsification attack over small network size, **h** MDR % during falsification attack over small network size, **i** Throughput % during falsification attack over small network size, **j** End-to-end delay during falsification attack over large network size, k MDR % during falsification attack over large network size, and **l** Throughput % during falsification attack over large network size

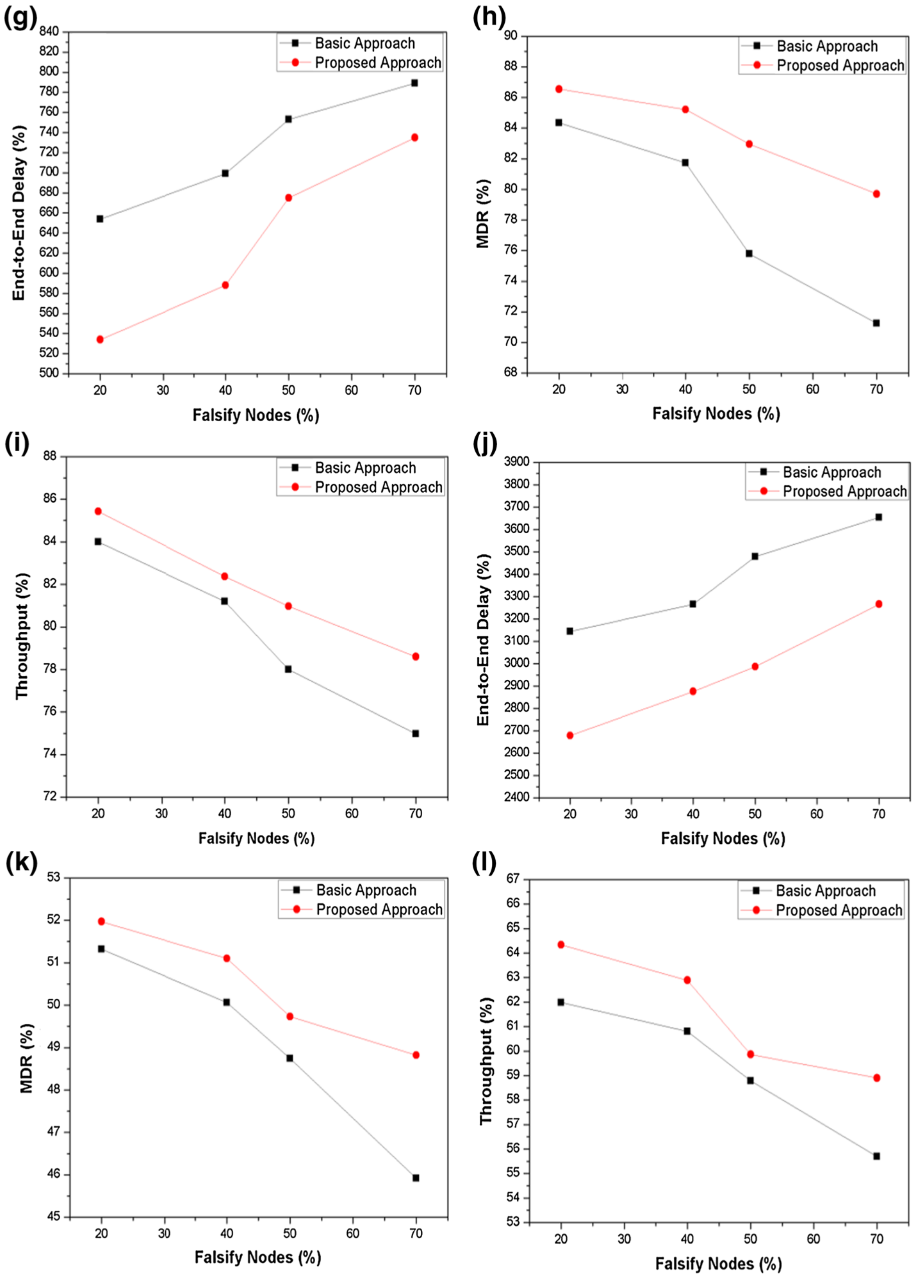

Fig. 5 continued

the attacks over small network sizes as depicted in Fig. 5b, c, h, 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.

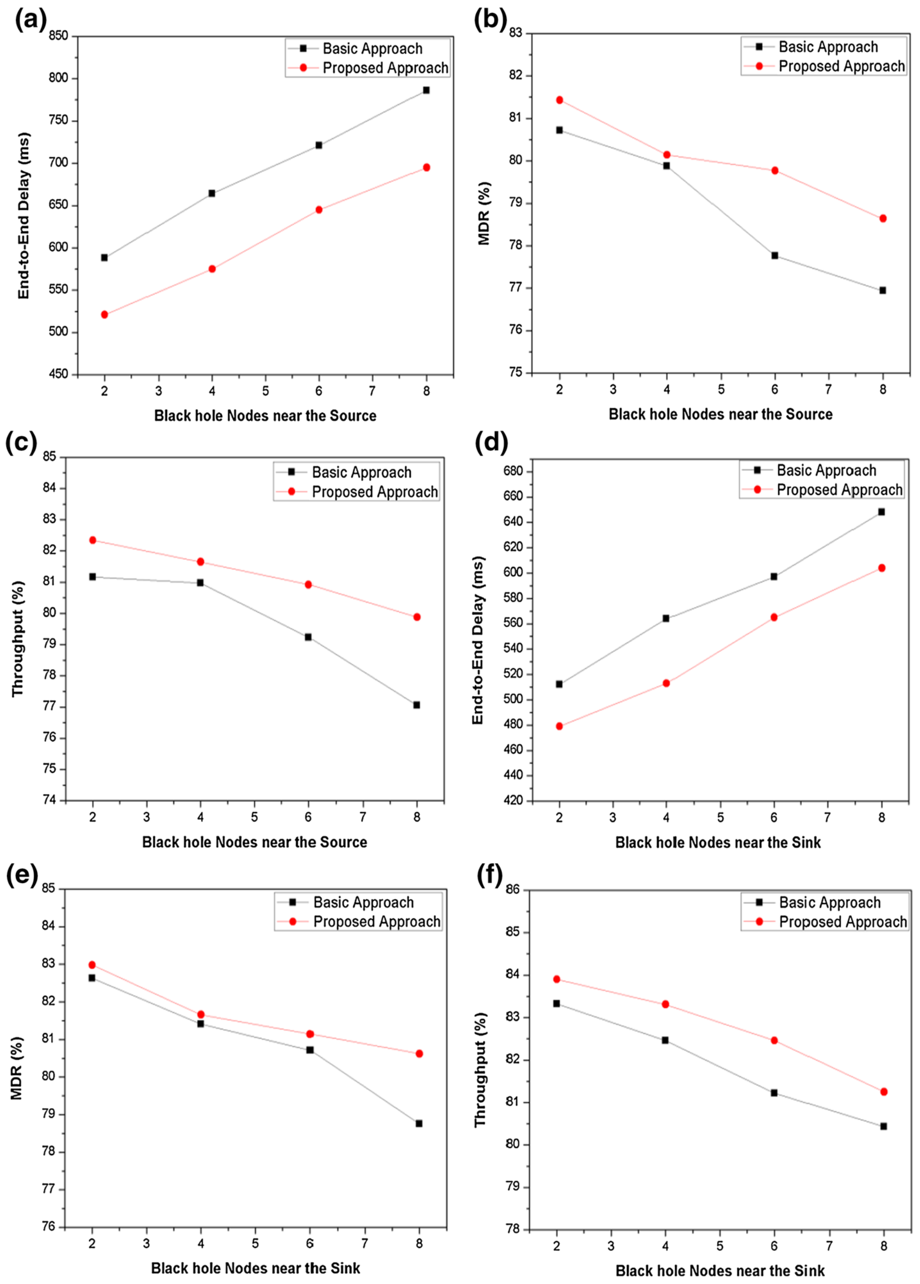

Fig. 6 Network metrics by increasing the number of black hole and falsify nodes near the source and sink nodes. **a** End-to-end delay over small network size, **b** MDR % over small network size, **c** throughput % over small network size, **d** end-to-end delay over large network size, **e** MDR % over large network size, **f** throughput % over large network size

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, Fig. 5g–l shows the results during falsification attack, the chances of falsification attack during the proposed approach reduce due to nodes' trust values while the basic approach may overcome the attacks through passive acknowledgement and two-hop information but may increase the time of path formation and packet transmission process. Therefore, the values of proposed approach are almost flat in large networks. By increasing the percentage of black hole and falsification attacks, in both the fixed and dynamic scenarios, the path recovery and packet transmission timings of basic approach increase because it identifies the attacker through passive acknowledgment process and applies the recovery process using two-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.

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 Fig. 6a–f shows the outcomes of network metrics by increasing the adversary nodes near the source and sink nodes. As the numbers of black hole nodes are increasing near the source and sink nodes, the end-to-end delay is increases but percentage of MDR and throughput are affected at a constant rate in the proposed mechanism.

To validate the proposed approach, Fig. 7a, b shows the experimental results of proposed and basic approach against end-to-end delay and MDR percentage. The experimental results are same as the simulated results through NS2 simulator. In a network size of 8 nodes, the experimental end-to-end delay of the proposed approach is 186 ms while through NS2 simulator the delay is 190 which is approximately same as experimental result. Similarly, the MDR percentage of the proposed mechanism is 97.53% through experimental and 97.50% using NS2 simulator. The proposed

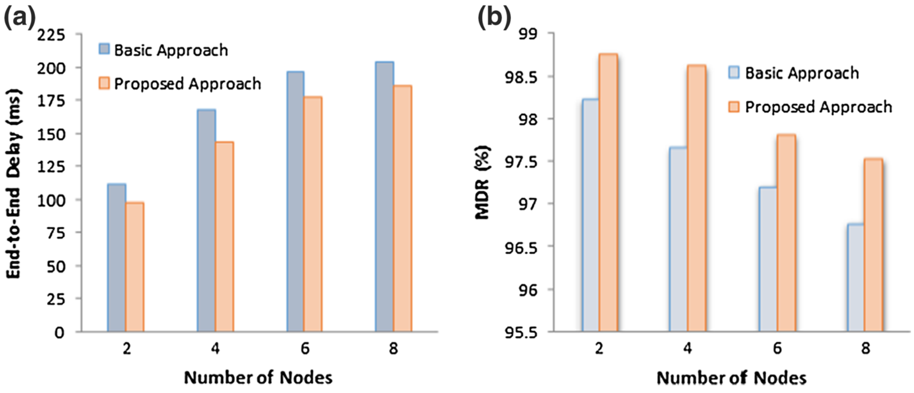

Fig. 7 Experimental results over increasing number of nodes. **a** End-to-end delay, **b** MDR %

mechanism significantly reduces the delay because of its fastest path formation process and packet transmission through trust factors. Further, the MDR percentage of the proposed mechanism also shows better results because of its positive weight computation through SITO.

6 Conclusion

In this paper, the WTR mechanism using SITO has been exploited to perceive and eliminate the malicious 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 supports 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 to that of the reported SRPM protocol. In addition to this, we have validated the proposed approach with experimental results at smaller values of the network size. However, the energy consumption in the large network sizes during the packet transmission/reception is a potential issue which will be reported in future communication.

Acknowledgements The authors are sincerely thankful to the anonymous reviewers for critical comments and suggestions to improve the quality of the manuscript.

References

1. Silva, L. C. D., Morikawa, C., & Petra, I. M. (2012). State of the art of smart home. *Engineering Applications of Artificial Intelligence, 25*(7), 1313–1321.
2. Coutaz, J., & Crowley, J. L. (2016). A first-person experience with end-user development for smart homes. *IEEE Pervasive Computing, 15*(2), 26–39.
3. Domaszewicz, J., Lalis, S., Pruszkowski, A., Koutsoubelias, M., Tajmajer, T., Grigoropoulos, N., et al. (2016). Soft actuation: smart home and office with human-in-the-loop. *IEEE Pervasive Computing, 15*(1), 48–56.
4. Namasudra, S., & Roy. P. (2015). Size based access control model in cloud computing. In *Proceedings of the IEEE international conference on electrical, electronics, signals, communication and optimization, Visakhapatnam* (pp. 1–4).
5. Gopalakrishnan, I. (2011). *Wireless mesh routing in smart utility networks*. Ph.D. Thesis, Auburn University.
6. Namasudra, S., Nath, S., & Majumder, A. (2014). Profile based access control model in cloud computing environment. In *Proceedings of the IEEE international conference on green computing, communication and electrical engineering, Coimbatore* (pp. 1–5).
7. Garzon, C., Camelo, M., Vila, P., & Donoso, Y. (2015). A multi-objective routing algorithm for wireless mesh network in a smart cities environment. *Journal of Networks, 10*(1), 60–69.
8. Iyer, G., Agrawal, P., & Cardozo, R. S. (2013). Performance comparison of routing protocols over smart utility networks: A simulation study. In *Proceedings of IEEE Globecom workshops (GC workshops), Atlanta, GA* (pp. 969–973).
9. Majumder, A., Namasudra, S., & Nath, S. (2014). Taxonomy and classification of access control models for cloud environments. In Z. Mahmood (Ed.), *Continued rise of the cloud* (pp. 23–53). London: Springer.
10. Mendes, T. D. P., Godina, R., Rodrigues, E. M. G., Matias, J. C. O., & Catalao, J. P. S. (2015). Smart home communication technologies and applications: Wireless protocol assessment for home area network resources. *Energies, 8*(7), 7279–7311.

11. Namasudra, S., Roy, P., Vijayakumar, P., Audithan, S., & Balamurugan, B. (2017). Time efficient secure DNA based access control model for cloud computing environment. *Future Generation Computer Systems*. doi:10.1016/j.future.2017.01.017.
12. Rehman, S. U., & Manickam, S. (2016). A study of smart home environment and its security threats. *International Journal of Reliability, Quality and Safety Engineering, 23*(3), 1–9.
13. Iyer, G., Agrawal, P., & Cardozo, R. S. (2013). Analytic model and simulation study for network scalability in smart utility networks. In *Proceedings of IEEE innovative smart grid technologies-Asia (ISGT Asia), Bangalore* (pp. 1–6).
14. Namasudra, S., & Roy, P. (2016). Secure and efficient data access control in cloud computing environment: A survey. *Multiagent and Grid Systems, 12*(2), 69–90.
15. Bala, S., Sharma, G., & Verma, A. K. (2016). PF-ID-2PAKA: Pairing free identity-based two-party authenticated key agreement protocol for wireless sensor networks. *Wireless Personal Communications, 87*(3), 995–1012.
16. Namasudra, S., & Roy, P. (2016). A new secure authentication scheme for cloud computing environment. *Concurrency and Computation: Practice and Exercise*. doi:10.1002/cpe.3864.
17. Huang, H., Gong, T., Chen, P., Malekian, R., & Chen, T. (2016). Secure two-party distance computation protocol based on privacy homomorphism and scalar product in wireless sensor networks. *Tsinghua Science and Technology, 21*(4), 385–396.
18. Jhaveri, R. H., & Patel, N. M. (2016). Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. *International Journal of Communication Systems*. doi:10.1002/dac.3148.
19. Anita, X., Bhagyaveni, M. A., & Manickam, J. M. L. (2015). Collaborative lightweight trust management scheme for wireless sensor networks. *Wireless Personal Communications, 80*(1), 117–140.
20. Labraoui, N., Gueroui, M., & Sekhri, L. (2016). A risk-aware reputation-based trust management in wireless sensor networks. *Wireless Personal Communications, 87*(3), 1037–1055.
21. Xi, C., Liang, S., Jian Feng, M. A., & Zhuo, M. A. (2015). A trust management scheme based on behavior feedback for opportunistic networks. *China Communications, 12*(4), 117–129.
22. Kerrache, C. A., Calafate, C. T., Cano, J. C., Lagraa, N., & Manzoni, P. (2016). Trust management for vehicular networks: An adversary-oriented overview. *IEEE Access, 4,* 1–15.
23. Namasudra, S., & Roy, P. (2017). A new table based protocol for data accessing in cloud computing. *Journal of Information Science and Engineering, 33*(3), 585–609.
24. Namasudra, S., & Roy, P. (2017). Time saving protocol for data accessing in cloud computing. *IET Communications*. doi:10.1049/iet-com.2016.0777.
25. Salima, S., Obaidat, M. S., Zarai, F., & Hsiao, K. F. (2015). A new secure and efficient scheme for network mobility management. *Journal of Security and Communications, Networks, 8*(7), 1360–1377.
26. Sun, L., Pinyi, R., Qinghe, D., & Yichen, W. (2016). Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics, 12*(1), 291–300.
27. Sultana, S., Ghinita, G., Bertino, E., & Shehab, M. (2015). A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks. *IEEE Transactions on Dependable and Secure Computing, 12*(3), 256–269.
28. Boushaba, M., Hafid, A., & Gendreau, M. (2016). Source-based routing in wireless mesh networks. *IEEE Systems Journal, 10*(1), 262–270.
29. Neumann, A., Lopez, E., Cerda, A. L., & Navarro, L. (2016). Securely-entrusted multi-topology routing for community networks. In *Proceedings of 12th annual conference on wireless on-demand network systems and services (WONS), Cortina d'Ampezzo* (pp. 1–8).
30. Talawar, S. H., & Ramesh, C. H. (2015). A protocol for end-to-end key establishment during route discovery in MANETs. In *Proceedings of 29th international conference on advanced information networking and applications (AINA), Gwangju* (pp. 176–184).
31. Benitez, Y. I. S., Ben, O. J., & Claude, J. P. (2014). Performance evaluation of security mechanisms in RAOLSR protocol for wireless mesh networks. In *Proceedings of IEEE international conference on communications (ICC), Sydney, June 2014* (pp. 1808–1812).
32. Wang, H., Chin, K., & Soh, S. (2016). On minimizing data forwarding schedule in multi transmit/receive wireless mesh networks. *IEEE Access, 4,* 1570–1582.
33. Darehshoorzadeh, A., Robson, G., & Azedine, B. (2015). Towards a comprehensive model for performance analysis of opportunistic routing in wireless mesh networks. *IEEE Transactions on Vehicular Technology*. doi:10.1109/TVT.2015.2457680.
34. Sbeiti, M., & Wietfeld, C. (2014). One stone two birds: On the security and routing in wireless mesh networks. In *Proceedings of IEEE wireless communications and networking conference (WCNC), Istanbul* (pp. 2486–2491).

35. Babu, M. R., & Usha, G. (2016). A novel honey pot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET. *Wireless Personal Communications, 90*(2), 831–845.
36. Poongodi, T., & Karthikeyan, M. (2016). Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks. *Wireless Personal Communications, 90*(2), 1039–1050.
37. Khan, S., Loo, K. K., Mast, N., & Naeem, T. (2010). SRPM: Secure routing protocol for IEEE 802.11 infrastructure-based wireless mesh networks. *Journal of Network and Systems Management, 18*(2), 190–209.
38. Khan, S., Alrajeh, N. A., & Loo, K. K. (2012). Secure route selection in wireless mesh networks. *Computer Networks, 56*(2), 491–503.
39. Rathee, G., & Saini, H. (2016). Weight trusted routing mechanism for hierarchical mesh environments. *International Journal of Distributed Systems and Technologies, 8*(3), 25–42.
40. Macas M., & Lhotska L. (2007) Social impact theory based optimizer. In: F. Almeida e Costa., L.M. Rocha., E. Costa., I. Harvey., A. Coutinho (Eds) *Advances in Artificial Life. ECAL 2007. Lecture notes in computer science*, vol. 4648, (pp. 635–644). Springer, Berlin.
41. Matti, T., & Jorma, S. (2001). Dijkstra's shortest path routing algorithm in reconfigurable hardware. In *Proceedings of 11th international conference on field-programmable logic and applications, Belfast, Northern Ireland* (pp. 653–657).

Geetanjali Rathee received B.Tech Degree in Computer Science and Engineering from Bhagwan Mahavir Institute of Engineering and Technology (BMIET), Haryana in the year 2011. She has completed her M.Tech in Computer Science and Engineering from Jaypee University, Waknaghat, Solan in the year 2014. She has submitted her Ph.D. thesis (viva-voce examination pending). Currently, she is working as an Assistant Professor in Computer Science and Engineering Department in Jaypee University, Waknaghat, Solan. Her research interest include resiliency in wireless mesh network, routing protocols, network protocols and security in next generation communication systems, security aspects in cognitive radio network.

Hemraj Saini is currently working as Assistant Professor (Senior Grade) in the Department of Computer Science and Engineering, Jaypee University of Information Technology, Waknaghat-173234 India. He has received his Ph.D. from Utkal University, Bhubaneswar, India in 2012, M.Tech. from Punjabi University, Patiala, India and B.Tech. from NIT Hamirpur, India in 2005 and 1999, respectively. He is having more than 16 years of teaching and R&D experience. He has published around 100 research papers in journals and conferences of international repute. He has organized National and International conferences sponsored by agencies like IEEE, CSI, AICTE, CSIR, DST etc. He is the member of different professional technical and scientific associations such as IEEE (Mem. No. 92738007), ACM (Mem. No. 5156611), IAENG (Mem. No. 133186), etc. Presently he is providing his services in various modes like, reviewer for different reputed journals and conferences and also the Member of Editorial boards and Technical Program Committees.

Professor Ghanshyam Singh received Ph.D. degree in Electronics Engineering from the Indian Institute of Technology, Banaras Hindu University, Varanasi, India, in 2000. He was associated with Central Electronics Engineering Research Institute, Pilani, and Institute for Plasma Research, Gandhinagar, India, respectively, where he was Research Scientist. He had also worked as an Assistant Professor at Electronics and Communication Engineering Department, Nirma University of Science and Technology, Ahmedabad, India. He was a Visiting Researcher at the Seoul National University, Seoul, South Korea. At present, he is Professor with the Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Waknaghat, Solan, India. He is an author/co-author of more than 200 scientific papers of the refereed Journal and International Conferences. His research and teaching interests include RF/ Microwave Engineering, Millimeter/THz Wave Antennas and its Applications in Communication and Imaging, Next Generation Communication Systems (OFDM and Cognitive Radio), and Nanophotonics. He has more than 17 years of teaching and research experience in the area of Electromagnetic/Microwave Engineering, Wireless Communication and Nanophotonics. He has supervised various Ph.D. and M.Tech. theses. He has worked as a reviewer for several reputed Journals and Conferences. He is author of two books "Terahertz Planar Antennas for Next Generation Communication" and "MOSFET Technologies for Double-Pole Four-Throw Radio-Frequency Switch" published by Springer.