Hindawi Publishing Corporation
Journal of Engineering
Volume 2016, Article ID 2089714, 9 pages
http://dx.doi.org/10.1155/2016/2089714

Research Article

Secure Trust Based Key Management Routing Framework for Wireless Sensor Networks

Jugminder Kaur, Sandeep S. Gill, and Balwinder S. Dhaliwal

Department of Electronics and Communication Engineering, Guru Nanak Dev Engineering College, Ludhiana 141006, India

Correspondence should be addressed to Jugminder Kaur; jugminder_3@yahoo.co.in

Received 19 September 2015; Revised 24 December 2015; Accepted 3 February 2016

Academic Editor: Gokhan Sahin

Security is always a major concern in wireless sensor networks (WSNs). Several trust based routing protocols are designed that play an important role in enhancing the performance of a wireless network. However they still have some disadvantages like limited energy resources, susceptibility to physical capture, and little protection against various attacks due to insecure wireless communication channels. This paper presents a secure trust based key management (STKF) routing framework that establishes a secure trustworthy route depending upon the present and past node to node interactions. This route is then updated by isolating the malicious or compromised nodes from the route, if any, and a dedicated link is created between every pair of nodes in the selected route with the help of "q" composite random key predistribution scheme (RKPS) to ensure data delivery from source to destination. The performance of trust aware secure routing framework (TSRF) is compared with the proposed routing scheme. The results indicate that STKF provides an effective mechanism for finding out a secure route with better trustworthiness than TSRF which avoids the data dropping, thereby increasing the data delivery ratio. Also the distance required to reach the destination in the proposed protocol is less hence effectively utilizing the resources.

1. Introduction

A WSN comprises battery-powered sensor nodes with extremely limited processing capabilities [1]. It covers a wide range of applications, including homeland security and personal healthcare, military surveillance, building and urban surveillance, industrial operations, and environmental monitoring. Their increasing penetration mainly stems from numerous advantages like wireless operation, low cost, easy installation, and self-organization [2]. These advantages, however, introduce security issues. The nodes need to cooperate in order to accomplish certain networking tasks (e.g., routing) to meet the random deployment requirement, introducing additional vulnerabilities. The wireless operation of WSNs renders them vulnerable to privacy attacks while the nodes low cost is closely related to low capabilities in terms of processing memory and energy resources, which limits the functionality that can be implemented to defend against the security attacks. In WSN, secure routing is more demanding due to the nature of the routing operation in WSN. Since WSN lacks an infrastructure, nodes depend on the cooperation among each other to route their packets. Thus, a router in WSN is simply any node that offers a routing service.

With the open and remote deployment environment, WSNs are generally susceptible to various attacks that are categorized below.

Depending upon the location of origin, the attacks can be divided into two types: internal and external. In internal attacks, an attacker obtains authorization to access the network whereas in external attacks; attackers are precluded from the network and have no right to access the network [3]. The attacks depending upon their nature can also be categorized as passive and active. In passive attacks, malicious nodes may gather sensitive information or behave selfishly in collaborative operations, such as routing, to passively affect the proper operation of WSNs. In active attacks, malicious nodes may actively request sensitive information, influencing the behaviour of surrounding nodes, or affecting the normal operation of WSNs using attacks such as denial of service [3].

Depending upon the behaviour of attacker node [4], common attacks can be illustrated as follows:

(i) Black hole attack in which a malicious node discards all the packets it should forward.

(ii) Grey hole attack in which an attacker drops certain type of packets (routing packets, data packets from a designated node, etc.) and forwards part of them.

(iii) Sinkhole attack is that in which a compromised node attracts nearly all the traffic from a particular area and disguises itself as a sink node.

(iv) Wormhole attack is a type of attack in which data packets received in one part of the network may be tunnelled by a pair of adversaries and will be replayed in another part through a low-latency link.

(v) In message tampering attack, a malicious node tampers the receiving message before forwarding it to other nodes [4].

Consequently, secure routing is very important to guarantee the network functionality in the presence of malicious or selfish nodes and to achieve it several routing protocols have been implemented from time to time. However, these routing protocols mainly rely on cryptographic primitives and authentication mechanisms which are not suitable for WSNs.

Trust Based Routing and Its Need. A trust aware routing protocol is a protocol in which a node incorporates its opinion about the behaviour of a candidate router in the routing decision. This opinion is quantified and called the trust metric. Route is established on the basis of trust metric from source to destination. Trust aware routing is important for securing obtained information, protecting the network performance from degradation and network resources from unreasonable consumption. Most WSN applications carry and deliver very critical and secret information like in military and health applications. WSN infected by misbehaving nodes misroute packets to wrong destination leading to misinformation or do not forward packets to the destination leading to loss of information. Having a trust aware routing protocol can protect data exchange, secure information deliver, and protect the value of communicated information. However, the traditional trust based routing protocols have some key problems. The trust based schemes deal with the inherent attacks in wireless networks but also induce some new risks to which special consideration should be given. Also most trust models do not consider the particularity of trust metrics when designing routing protocols and the existing trust based routing protocols have some limitations like dependence on specific routing scheme means the security mechanisms become invalid if the routing protocol of the network will be changed [4].

"q" Composite RKPS. Generally in basic RKPS scheme, any two neighbour nodes find a single common key from their key rings and establish a secure link. In "q" composite RKPS, "q" (>1) common keys are used. As the amount of required key overlap increases, it becomes exponentially harder for an attacker with a given key set to break a link. Hence, we can say that, by increasing the amount of key overlap required for key-setup, resiliency of the network against node capture is increasing [5].

In this paper, we have proposed STKF to enhance the security of the route and ensure the data delivery to the destination. For this, a hybridization of TSRF and "q" composite RKPS is done in order to achieve security and surety under malicious environment. Firstly the route is found on the basis of trust values calculated by the direct and indirect interaction of nodes with each other keeping distance threshold. The proposed routing protocol is then updated and made immune to every type of attack. For this, the route found on the basis of TSRF is scanned for malicious nodes and the malicious nodes found are replaced by the well behaved nodes in the same level which eliminate the possibility of any internal attack. The nodes are then arranged in an order with least distance to the receiver and maximum trust value. After updating the route, a dedicated link is created between each pair of nodes to transfer the data hence eliminating any possibility of external attack. Therefore, the delivery ratio will not degrade and will remain maximum any type of attack may occur. The proposed routing protocol is then compared with TSRF and it has been found that the trust value of the updated route increases making the route more trustworthy. Also the distance required to reach the destination decreases in the proposed routing protocol.

The rest of the paper includes related work, description, and implementation of STKF and performance evaluation.

The rest of the paper is organized as follows: Section 2 includes related work, description and implementation of STKF are given in Section 3, and performance evaluation is done in Section 4.

2. Related Work

Several routing frameworks have been proposed over years to establish a secure route. Greedy Perimeter Stateless Routing (GPSR) [6] is a novel routing protocol for wireless datagram networks that makes greedy forwarding decisions using only information about a router's immediate neighbours in the network topology. It scales better in per-router state than shortest-path and ad hoc routing protocols as the number of network destinations increases. However this protocol is not able to provide any kind of security against attacks.

SAODV [7] which is a security extension of AODV protocol is implemented to resist against some routing attacks. In this, a mechanism called double signature is introduced which increases the load of intermediate nodes. A-SODV [8] is then developed to overcome the negative effects of SAODV but these protocols are not suitable for resource constrained WSNs.

The trend of trust based routing has emerged in recent years to improve the security of WSN. A secure dynamic source routing protocol [2] is implemented for mobile sensor network by incorporating trust based mechanism in existing DSR. The trust model uses the inherent features of DSR protocol to derive and compute the respective trust levels in other nodes. This protocol is based upon trust update interval (TUI) which determines the time a sending node must wait after transmitting a packet and update a trust value depending

upon the response. However this protocol is able to deal with certain types of attacks.

Yu et al. [9] analyzed various attacks and countermeasures related to trust schemes in WSNs. However, they did not design secure routing protocol according to analysis result. Zahariadis et al. [10], Zhang et al. [11], and Crosby et al. [12] proposed several trust based routing protocols that play an important role in improving the security of WSNs but they are confined to specific routing schemes which restricts the scope of application.

3. Material and Methods

3.1. STKF Network Model. In this paper, the proposed protocol is designed for a generalized communication model that can be implemented for a variable number of nodes and for large as well as small WSNs. The initial step is to create the network environment by defining the network parameters which includes area for deploying sensor network, number of nodes in the network, proportion of malicious nodes in network if considering the effect of attacks, and transmission range over which a node can communicate. We have designed a WSN with number of sensing nodes varying from 50 to 100 that are distributed over an area of $100 \times 100\,\mathrm{m}^2$ and $200 \times 200\,\mathrm{m}^2$ randomly or manually. The proportion of malicious nodes varies from 10% to 50% in the network. Moreover, any node in a system can initiate a routing operation and any other node can be a destination for that node. The selection of the source-destination pair is done randomly. Each sensor node is in charge of both detecting events and acting as a router in order to forward packets. All the sensor nodes are resource constrained and have the same limited radio coverage. The reason of adopting this model is to study a very general case and not limiting our scope to particular scenarios.

3.2. Neighbour Selection in STKF. Neighbour selection in a WSN is a very crucial part as the neighbour nodes are responsible for routing the data from source to destination. So the neighbours must be selected effectively in order to find an efficient route. Here the factors taken under consideration for neighbour selection are distance and trust relations.

(i) Once the source and the destination nodes are defined, source node will start searching for its neighbour nodes. The source node will broadcast a distance request signal containing source address in a network.

(ii) All the nodes except the source node will then acknowledge the source node with a distance metric and its address. Here the distance of every other node from the source node is found by Euclidean's distance formula (Distance vector approach).

For two nodes, node "i" with coordinates x_1, y_1 and node "j" with coordinates x_2, y_2, the distance of node "j" from node "i" is calculated as below:

$$D(i,j) = \sqrt{\left[(x_1 - x_2)^2 + (y_1 - y_2)^2\right]}. \quad (1)$$

(iii) Upon receiving the acknowledgment, source node will select the neighbour node below threshold which means the nodes with distance less than the threshold defined will be taken as neighbour nodes.

Threshold area for finding out neighbour nodes = length of monitoring area/2.

It is to be noted here that the threshold area is dependent on the dimensions of the network.

3.3. Route Establishment Using TSRF Implementation. The next hop selection among the neighbours defined is done on the basis of trust based routing protocol in which overall trust value for each node is calculated on the basis of direct and indirect interactions of any node with the source node and neighbouring nodes.

(i) For selecting the next hop, source node will send a trust request signal (containing source address) to the selected neighbour nodes.

(ii) The neighbour nodes acknowledge the source node with trust reply which contain the neighbour node's ID and overall trust metric.

The overall trust will be computed by the neighbour node for a source node as

$$t(i,j)^l = \alpha \mathrm{dt}(i,j)^l + \beta \frac{\sum_{(k \in Cj, k \neq i)}^{n} \mathrm{it}(k,j)^l}{n-1}. \quad (2)$$

Here $t(i, j)$ represents the trust value of node j for node i. $\mathrm{dt}(i, j)$ is the direct trust value of node j for node i. $\mathrm{it}(k, j)$ stands for the recommendations provided by node k which belongs to the neighbour set of node j. n denotes the number of neighbours. l represents the sequence number of the evaluation records. α and β are weighed factors related to security policies whose values are 0.7 and 0.3, respectively.

A larger value of α indicates that the sensor node in WSNs is more convinced about its own judgement and a larger value for β indicates that the recommendations provided by other nodes are more trustworthy in trust evaluation process.

(iii) Direct trust (dt) is obtained from the present and past direct interactions of neighbour nodes with source node which will be stored in the memory of every node.

It is to be noted here that direct trust value of a node with every other node is a database of one node which is updated regularly after every success or failure communication and the value of it is computed as

$$\mathrm{dt}(i,j)^l = \gamma_1 \mathrm{dt}_{P(j)}(i,j)^{l-1} + \gamma_2 \mathrm{dt}_{N(j)}(i,j)^{l-1} + ids(i,j)^l. \quad (3)$$

Here, $\mathrm{dt}_{P(j)}(i, j)^{l-1}$ represents the direct trust value of node j for node i based upon node j's past well behaved behaviour; $\mathrm{dt}_{N(j)}(i, j)^{l-1}$ represents the direct trust value of node j for node i based upon node j's past malicious behaviour. γ_1 and γ_2 correspond to the exponential decay time factor of the positive and negative assessment, which is taken as 0.90 and 0.99, respectively. $ids(i, j)^l$ denotes the assessment for current

behaviour of device j by utilizing intrusion detection systems which is given by

$$ids(i,j) = \begin{cases} P(j), & 0 < P(j) < 1 \\ 0, & \text{uncertain} \\ N(j), & -1 < N(j) < 0. \end{cases} \quad (4)$$

Here, $P(j)$ and $N(j)$ represents the positive and negative assessment for device j's behaviour, respectively.

The value of $P(j)$ is kept constant as 0.01 which is responsible for developing good reputation of a node and $N(j)$ as −0.1, which is responsible for developing bad reputation of a node. By keeping these values, a node has to perform well most of the time for obtaining a good reputation (direct trust value high) as the effect of $P(j)$ is kept less as compared to $N(j)$.

(iv) Indirect trust (it) stands for the trust relations between distributed nodes without direct interactions. Indirect trust value for any neighbouring node is collected from its neighbouring nodes (except the evaluating node).

For instance, if j is the neighbour node of i which is a source node, the indirect trust for j is its past behaviour (direct interaction) with its neighbour nodes $(k, l, m, \ldots)$ with the source node (evaluating node) and the past behaviour of neighbours $(k, l, m, \ldots)$ of neighbour node j with the source node which will be present in the database of respective nodes $(k, l, m, \ldots)$ and is exchanged with the help of request reply messages.

The indirect trust value is computed as

$$\sum_{(k \in Cj, k \neq i)}^{n} \mathrm{it}(k,j)^l \equiv \sum_{(k \in Cj, k \neq i)}^{n} \left(\mathrm{dt}(i,k)^l \, \mathrm{dt}(k,j)^l \right). \quad (5)$$

Here $\mathrm{it}(k, j)$ represents indirect trust value of node j for node k. $\mathrm{dt}(i, k)$ stands for direct trust value of node k for node i. $\mathrm{dt}(k, j)$ represents the direct trust value of node j for node k that provides the recommendation data.

Depending upon the value of overall trust metric, trust value of neighbour nodes is computed and the node with the maximum trust value among them is selected as next node. The process continues until the route has reached the destination node. Then the nodes from source node to next node to destination nodes are stored to create a routing table and the route is discovered.

Overall trust value of the path is calculated by taking the product of trust values of nodes in the route.

3.4. Route Update: Enhanced TSRF. TSRF is a very secure routing protocol but its performance varies with respect to the extent of faulty environment, hence degrading delivery ratio. Enhancement over TSRF is done to create a fault-free environment which is implemented below:

(i) As we know attackers can degrade the performance of any sensor network by compromising the route nodes. Hence to find out a reliable route to destination, the malicious nodes need to be eliminated from the route. As we know overall trust value of any node depends upon the direct and indirect trust computations and because we are giving more significance to the direct trust value, false recommendations from the neighbour node can help the malicious node to find the place in the route. For this reason, the route found based upon TSRF is scanned for any malicious node in the route. If any node in the discovered route is found to be malicious, it will be replaced by the node with second maximum trust value in the same level.

(ii) The route is again updated by finding out the node (among the nodes in the previously defined route) closest in distance from the transmitter with maximum trust value, hence decreasing the overall distance covered and maximizing the trust value of path with least number of nodes required to reach the destination.

(iii) As the malicious nodes are eliminated in the updated route, no data dropping occurs hence maintaining data delivery ratio to 100%.

In this paper, the effect of attack on data delivery has been studied for TSRF and STKF. Here for a case, grey hole attack is taken in which an attacker node drops certain type of packets (routing packets, data packets from a designated node, etc.) and only forwards part of them due to which the delivery ratio drops by 50%.

3.5. Hybridization of Enhanced TSRF with "q" Composite RKPS. By demonstrating the concepts of getting route from source to destination with maximum trust and less data drop, intended security has been achieved but data surety is still a constraint. There is a one major problem for the present communication systems that is defined as hacking. As we have finally updated the route with no malicious node in it and data can now be transmitted from source to destination node on this discovered route, but there may exist malicious nodes in the network which can compromise any node in the route. So a dedicated link is created between transmitter and receiver which is basically a set of dedicated links between two neighbour nodes each time data transfers from source to destination. This dedicated link is created with the help of "q" composite RKPS. In this, any two neighbour nodes need to find "q" common keys where "q" is always greater than one among n length sequence, to establish a secure link in the key-setup phase. By increasing the amount of key overlap required for key-setup, we have increased the resilience of the network against node capture [13]. This approach is implemented in the steps below:

(i) In the initialization phase, we pick a set "S" of random keys out of the total key space and the sequence of keys is generated randomly until the keys at two ends do not match. For each node, we select "m" random keys from "S" (where "m" is the number of keys each node can carry in its key ring) and store them into the node's key ring [13].

(ii) While calculating the critical parameter $|S|$, the size of the key pool, it has to be kept in mind that key

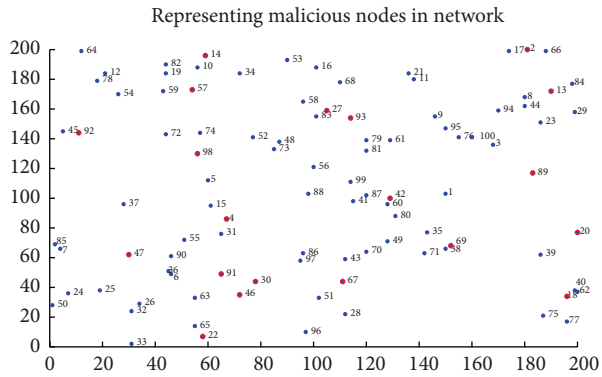

Figure 1: Representation of nodes deployed in WSN.

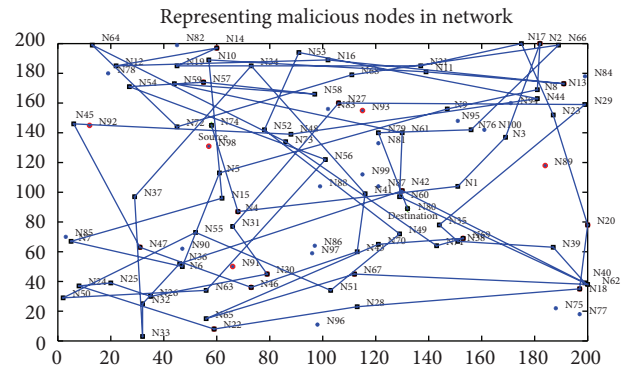

Figure 2: Route finding based upon TSRF.

pool size should not be too large, because then the probability of any two nodes sharing at least "q" keys will be very small which may take more than enough time to match the keys hence increasing the simulation time, and it should not be too small, because then we are unnecessarily sacrificing security.

(iii) In this paper we have taken set of 100 keys each of length 8. When the "q" (=5) number of keys (more than 60%) matches between two neighbouring nodes, a dedicated link is created between two nodes.

(iv) In the key-setup phase, once keys get matched between a pair of nodes, the transmitter will create a dedicated virtual path. The data to be transmitted is locked with the key matched and only the intended receiver with the same key sequence will unlock it.

(v) In key establishment phase, the data transmission from the transmitter node to the next node in the selected route with key approaching dedicational path is done.

(vi) This process continues from one node to other until the data reaches the destination point or the receiver.

(vii) Finally the performance of the designed protocol is studied for various parameters like effect on packet delivery ratio, performance under varying malicious environment, and effect of various attacks on packet delivery ratio.

4. Results and Discussions

To evaluate the performance of STKF, we simulate the code using MATLAB.

In our implementation, we have taken two examples for setting WSN. One is with 60 nodes deployed in a $100 \times 100\ m^2$ area and other is 100 nodes deployed over $200 \times 200\ m^2$ area. All other parameters are kept constant and their values are given in Table 1. However the nodes and the area can also be varied depending upon the network requirements in order to use the resources efficiently. But the number of nodes and area should be varied in proportion as more node deployment in small area will waste the resources and less nodes in large area will create coverage problem.

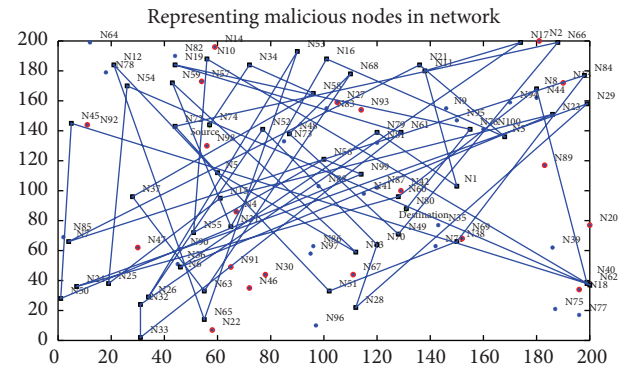

Figure 3: Route finding based upon STKF.

Table 1: Simulation parameters.

Parameters	Values
Monitoring area	$100 \times 100\ m^2$ and $200 \times 200\ m^2$
Number of nodes	60 and 100
Communication range	100 m
Threshold range	length/2
Routing protocol	TSRF
Initial trust level	0.5
Initial distrust level	0.5
Proportion of malicious nodes	(10–50)%
$P(a)$, $N(a)$	0.01, −0.1
α, β	0.7, 0.3
γ_1, γ_2	0.90, 0.99

Figures 1, 2, and 3 indicate deployment of 100 sensor nodes over $200 \times 200\ m^2$ with 20% malicious node in the network. The sensor nodes are randomly deployed in the given area.

Figure 1 represents the deployment of sensor nodes with blue dots indicating well behaved nodes and red dots indicating 20% malicious nodes.

Figure 2 represents route finding based upon TSRF in which route is found on the basis of trust values of nodes. The node with maximum trust value along the neighbours is selected as the next node in the route. However, some

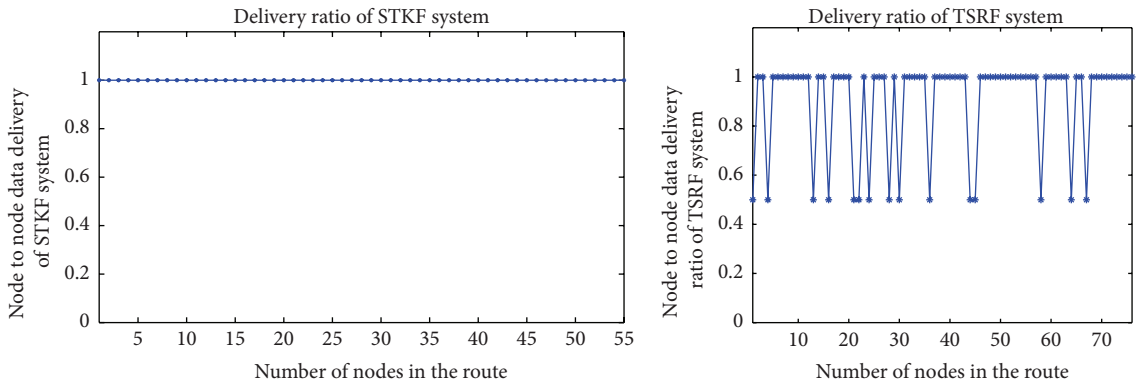

Figure 4: Graph representing comparison of delivery ratio.

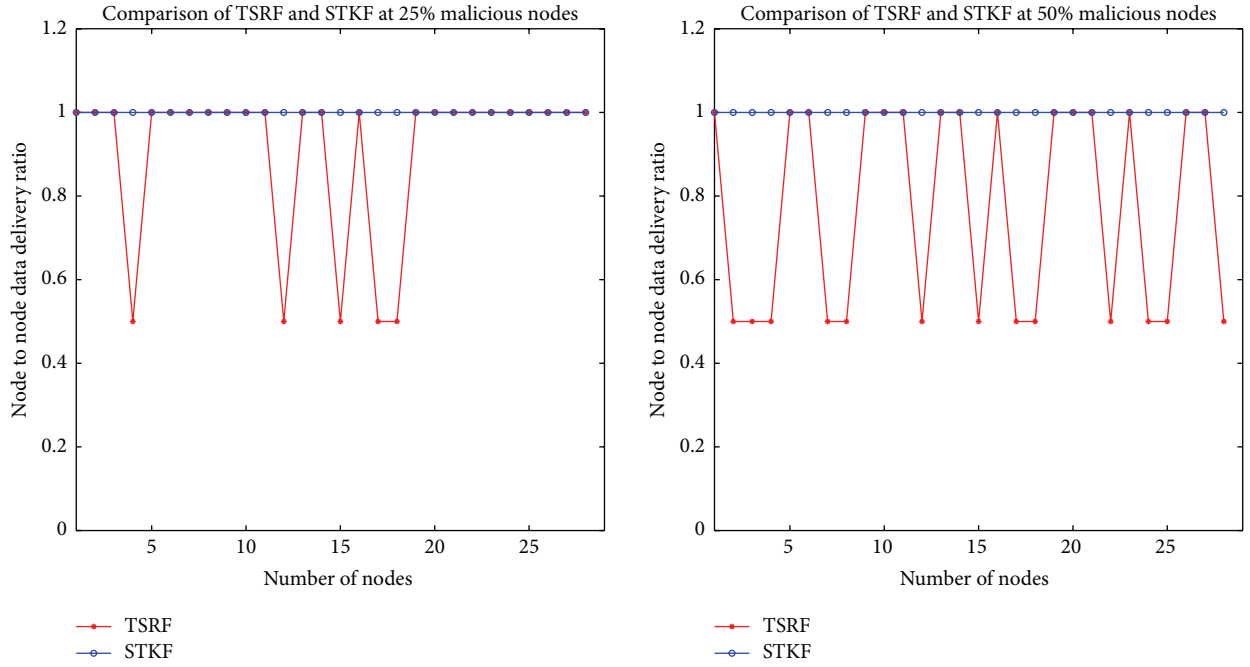

Figure 5: Graphs representing comparison of STKF and TSRF with 25% and 50% of malicious nodes deployed.

malicious nodes may get introduced due to false recommendations provided by other nodes. Hence those malicious nodes with larger trust values are participating in data transmission which deteriorate the route performance and hence delivery ratio.

Figure 3 illustrates route finding based upon advanced TSRF or STKF in which malicious nodes are replaced by the second maximum trust values in the node and then route is then simplified by arranging the nodes in the order to have less distance with maximum trust value as less energy will be needed for transferring the data between two nodes that are close to each other.

Figure 4 represents a graph indicating the comparison between the data delivery of STKF (Proposed) with the TSRF (old) routing protocol. Here x-axis represents the number of nodes in the route and y-axis is representing the node to node delivery ratio. Data in TSRF drops by 50% every time a malicious node (grey hole attack which drops the data by 50%) occurs in the route but data flows remain stable in STKF as malicious nodes have been overcome ensuring 100% delivery ratio.

Figure 5 represents the graphs indicating the comparison of both the routing protocols in varying environments. The data delivery ratios of TSRF (old) and STKF (proposed) are shown for 25% and 50% malicious nodes by keeping all other parameters like number of nodes in the network, area of the deployed network constant. When the proportion of malicious nodes in the network is more (50%), the probability of data dropping in the route found in TSRF increases. Hence the route will be less secure in TSRF. But as in STKF, malicious nodes have overcome; no data drop occurs at any node, hence maintaining a significant level of delivery ratio.

Figure 6 represents the graph indicating the comparison of node to node delivery ratio (y-axis) with respect to number

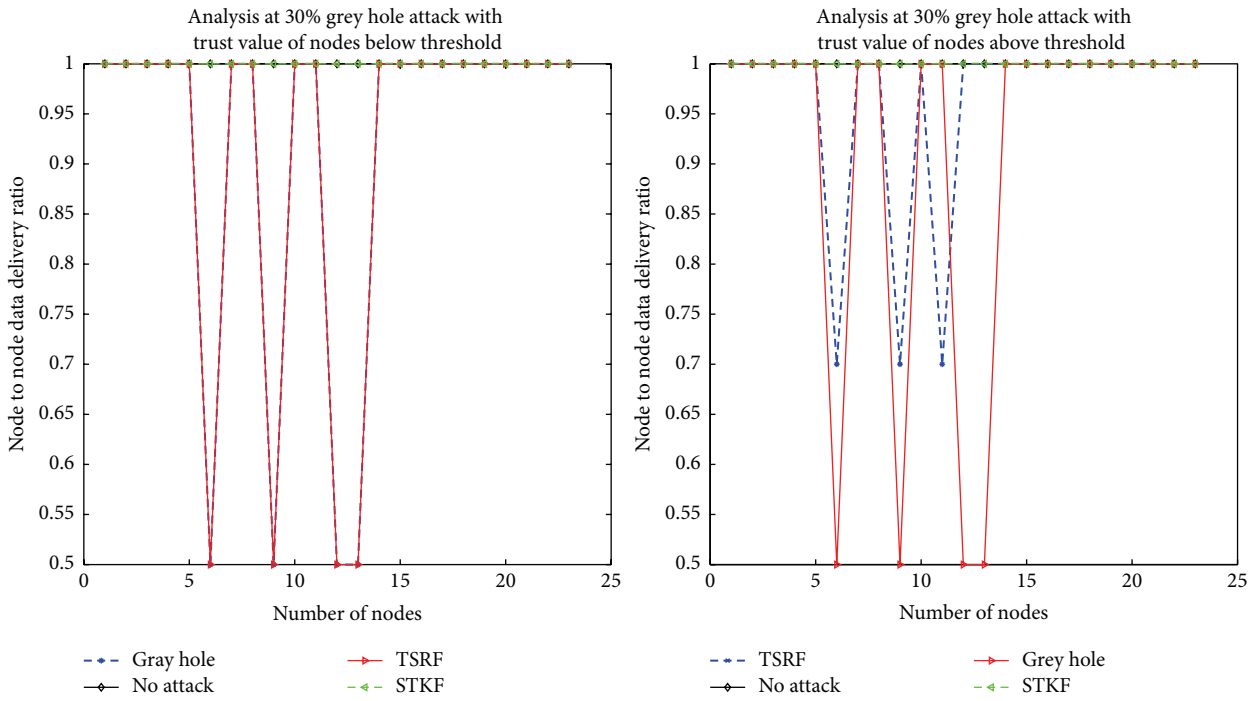

FIGURE 6: Graphs representing effect of trust value on the performance of TSRF and STKF routing protocols when trust value of nodes is below and above threshold.

of nodes in the route (x-axis). The comparison is done for overall trust value of path. It has been shown that when no attack occurs (black), data delivery ratio is maintained constant to 100%. When proportion of malicious node for grey hole attacker is taken as 30% (red curve), node to node data delivery ratio will be 0.5 at every grey hole attacker node. In the first graph when the trust value is below threshold (0.4), the performance of TSRF (blue curve) degrades to 0.5 at every malicious node and when the trust value is above threshold (0.4), the delivery ratio of TSRF (blue curve) increases (0.7). But the delivery ratio of STKF (green curve) is maintained and remains 100% even in the presence of 30% malicious nodes as in STKF once malicious nodes are overcome by trust worthy nodes, data will not drop.

Also it has to be kept in mind here that the proportion of malicious nodes is set to 30% with 100 number of nodes deployed over 200 × 200 m^2 area with all other parameters specified in the simulation table to be kept constant.

Table 2 represents the comparison of STKF and TSRF for the distances covered from source node to destination node, trust values of paths followed by them, and the time taken by both the protocols to find route. The algorithm is simulated for 100 and 60 number of nodes with areas 200 × 200 m^2 and 100 × 100 m^2, respectively. Four cases with different source node and destination node are taken for each set of nodes. In the first case with 100 nodes deployed randomly over the area of 200 × 200 m^2, it has been analyzed that the trust value of STKF (proposed) increases by 4.1×10^{-23}, 4.6×10^{-04}, 8.5×10^{-02}, and 1.9×10^{-07} than TSRF and distance required to reach the destination decreases by 1097 m (42%), 0363 m (61%), 1409 m (73%), and 0055 m (51%). When both the protocols are implemented for 60 nodes over the area of 100 × 100 m^2, the trust value of the route with STKF increases by 2.6×10^{-04}, 2.0×10^{-03}, 1.0×10^{-07}, and 3.2×10^{-08} compared to TSRF and distance decreases by 20 m (13%), 1 m (0.60%), 390 m (57%), and 432 m (61%). The time required to establish route in case of STKF decreases by 0.262, 0.258, 0.362, and 0.600 sec for 100 nodes and 0.338, 0.151, 0.260, and 0.349 sec for 60 nodes, respectively.

Table 3 shows the comparison of data delivery ratio with respect to percentage of malicious node for TSRF and STKF. It has been analyzed that, for a fixed trust value of path, delivery ratio for TSRF decreases with increase in percentage of malicious nodes while it remains constant for STKF which proves that STKF becomes immune to attacks once malicious nodes are replaced by well behaved nodes. Figures 7 and 8 represent the comparison of data delivery ratios of STKF and TSRF with respect to number of malicious nodes with different trust values of paths. Here 60 nodes are deployed evenly over an area of 200 × 200 m^2 keeping source (11) and destination (30) nodes fixed. It can be seen that data delivery ratio decreases from 43% to 10% for path trust value of 1.3×10^{-11} and 78% to 23% for path trust value of 0.0027 with increase in number of malicious nodes from 02 to 10 for TSRF. The data delivery ratio remains 100% for STKF as malicious nodes are replaced by well behaved nodes and it has been assumed that once malicious nodes have been overcome, data will not drop anywhere. It is to be noted that STKF performs well up to 50% proportion of malicious node which means it can deliver significant level of information even if half of nodes deployed get compromised in the network.

Table 2: Implementation results for conventional TSRF [4] and proposed STKF.

S. number	Source node	Destination node	Distance covered (m)		Trust value of path		Time taken to establish route (sec)	
			TSRF	STKF	TSRF	STKF	TSRF	STKF
Case 1: for number of nodes = 100, area of WSN = $200 \times 200\ m^2$								
1	10	74	2564	1467	7.7×10^{-38}	4.1×10^{-23}	0.830	0.568
2	10	98	0591	0228	2.2×10^{-11}	4.6×10^{-04}	0.383	0.125
3	20	10	1918	0509	4.1×10^{-05}	8.6×10^{-02}	0.435	0.073
4	28	64	0106	0051	6.5×10^{-16}	1.9×10^{-07}	0.903	0.303
Case 2: for number of nodes = 60, area of WSN = $100 \times 100\ m^2$								
5	07	12	0148	0128	7.2×10^{-04}	9.8×10^{-04}	0.483	0.145
6	11	08	0156	0155	7.0×10^{-03}	9.0×10^{-03}	0.233	0.082
7	11	29	0673	0283	2.2×10^{-11}	1.0×10^{-07}	0.400	0.140
8	12	30	0710	0278	1.1×10^{-11}	3.2×10^{-08}	0.494	0.145

Table 3: Comparison of data delivery ratio with respect to percentage of malicious node.

S. number	Percentage (%) of malicious nodes	Number of malicious nodes in the route	Data delivery ratio (%)			
			Case 1		Case 2	
Number of nodes = 60, area = $200 \times 200\ m^2$, Source node = 11, destination node = 30			TSRF with trust value = 1.3×10^{-11}	STKF with trust value = 1.4×10^{-07}	TSRF with trust value = 0.0027	STKF with trust value = 0.0300
1	10	02	43	100	78	100
2	20	04	32	100	65	100
3	30	05	30	100	58	100
4	40	10	13	100	41	100
5	50	12	10	100	23	100

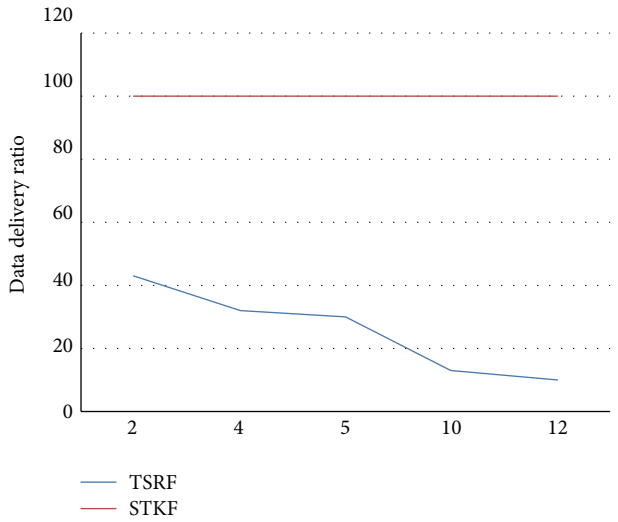

Figure 7: A graph between data delivery ratio and number of malicious nodes in the route (TSRF with trust value = 1.3×10^{-11} & STKF with trust value = 1.4×10^{-07}).

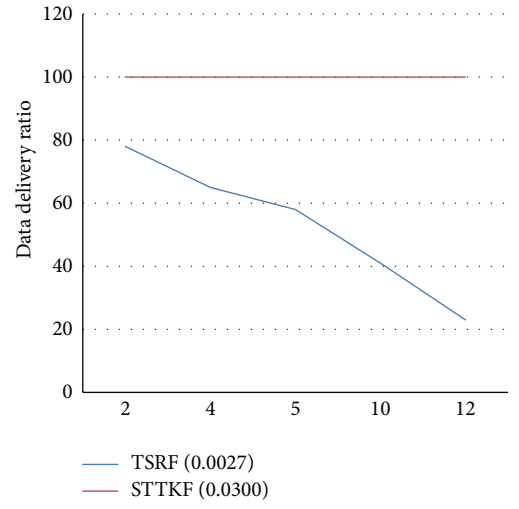

Figure 8: A graph between data delivery ratio and number of malicious nodes in the route (TSRF with trust value = 0.0027 & STKF with trust value = 0.0300).

It is to be noted here that this is the case for 60 nodes deployed keeping source (11) and destination (30) nodes fixed. It can be seen that data delivery ratio decreases with increase in number of malicious nodes for TSRF while it remains constant for STKF as in this malicious nodes are replaced by well behaved nodes. Also the data delivery is ensured by "q" composite RKPS which will provide acknowledgment every time data transfers between two intended nodes hence eliminating the terror of any external attacker.

5. Conclusion and Future Work

After implementing the concept of secure trust based key management routing framework, route established is more reliable, more trustworthy, and more secure as the trust value of the route in the proposed framework is more than the conventional trust based routing protocol. The following has been concluded:

(i) It has been analyzed that average trust value of STKF (proposed) increases by 0.58 and 1.2 than TSRF, when deploying 100 and 60 nodes over the area of $200 \times 200\ m^2$ and $100 \times 100\ m^2$, respectively.

(ii) Also the distance required to reach the destination node in the STKF is less than what was required by TSRF. The average percentage decrease in distance is 56.70% and 32.60% when deploying 100 and 60 nodes over an area of $200 \times 200\ m^2$ and $100 \times 100\ m^2$, respectively.

(iii) The data delivery ratio of STKF is also better than TSRF. The percentage of malicious nodes is varied from 10 to 50% and it has been analyzed that the average data delivery ratio remains 100% for the proposed protocol while it is 25.60% (low path trust value) and 53.00% (high path trust value) for TSRF.

In the future, we plan to decrease the routing overhead to reduce the energy consumption in order to make the routing protocol highly efficient. This will ultimately increase the network lifetime as the sensors are battery powered. In addition, the time required to establish a complete link between transmitter and receiver can be reduced in order to achieve faster communication.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors are thankful to the Director of Guru Nanak Dev Engineering College, Ludhiana (India), for providing support to accomplish the presented work.

References

[1] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: a trust-aware routing framework for WSNs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 184–197, 2012.

[2] P. Samundiswary and P. Dananjayan, "Secured reactive routing protocol for mobile nodes in sensor networks," *WSEAS Transactions on Communications*, vol. 9, no. 3, pp. 216–225, 2010.

[3] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, pp. 6–28, 2008.

[4] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: a trust-aware secure routing framework in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 209436, 14 pages, 2014.

[5] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 197–214, Berkeley, Calif, USA, May 2003.

[6] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, pp. 243–254, ACM, Boston, Mass, USA, August 2000.

[7] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM Workshop on Wireless Security*, pp. 1–10, Atlanta, Ga, USA, September 2002.

[8] D. Cerri and A. Ghioni, "Securing AODV: the A-SAODV secure routing prototype," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 120–125, 2008.

[9] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 867–880, 2012.

[10] T. Zahariadis, H. Leligou, P. Karkazis et al., "Design and implementation of a trust-aware routing protocol for large WSNs," *International Journal of Network Security & Its Applications*, vol. 2, no. 3, pp. 52–68, 2010.

[11] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM '10)*, pp. 1–9, San Diego, Calif, USA, March 2010.

[12] G. Crosby, N. Pissinou, and K. Makki, "Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks," *International Journal of Network Security*, vol. 12, no. 2, pp. 107–117, 2011.

[13] H. Chan, V. D. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 3, pp. 233–247, 2005.