Wireless Personal Communications (2019) 107:1799–1814
https://doi.org/10.1007/s11277-019-06357-3

Secure and Trust-Aware Routing Scheme in Wireless Sensor Networks

Azam Beheshtiasl[1] · **Ali Ghaffari**[1]

Published online: 9 April 2019

Abstract
Secure and trustable routing is one of the remarkable challenges in wireless sensor networks (WSNs). In this paper, we proposed a secure, trustable and energy-efficient routing method for WSNs. The proposed scheme uses Fuzzy logic to obtain the trust values of the routes. Then, the shortest route from the source to the destination was selected by considering trust and security. The proposed method uses the multidimensional scaling-map (MDS-MAP) optimal routing approach and measures the trust model via fuzzy logic. The proposed method was compared with Trust and Centrality degree Based Access Control (TC-BAC) and Trust-Aware Routing Framework (TARF) protocols. Through simulation experiment result, we show that the proposed scheme performs better than TC-BAC and TARF methods in terms of average packet delivery rate, average end-to-end delay and consumption energy.

Keywords WSNs · Trust model · Secure routing · Security · Fuzzy logic

1 Introduction

WSNs are made of a number of sensor nodes which receive data from the environment and transmit them to the sink hop by hop [1, 2]. Due to the extensive spread and the dynamic nature of WSNs, routing protocols are vulnerable to different attacks [3]. Such attacks are divided into internal and external attacks. Internal attacks are initiated by the compromised or malicious nodes and external attacks are initiated by those malicious nodes which do not have access to the network [4, 5]. For protecting WSNs against malicious and selfish behaviors, many different routing protocols have been developed [6, 7]. Common secure protocols can resist ageist some external attacks based on encryption but they cannot resist against malicious behaviors of internal nodes [8–11]. For defending a network against routing attacks in WSNs, especially against internal attacks, an alternative and efficient method i.e. trust management system, has been introduced which can detect a wide range of attacks. Nevertheless, it should be noted that the available trust management plans which have been designed for other networks are not suitable for WSNs since they consume a great deal of

✉ Ali Ghaffari
A.Ghaffari@iaut.ac.ir

[1] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

energy and memory. Trust models can effectively help network in distinguishing malicious nodes from normal nodes. In addition to helping network nodes to self-organize themselves with respect to the changes occurred in their neighborhood, trust models can participate in establishing and maintaining security protocols [12]. Different trust-based prevention protocols such as encryption, authentication and key management have been used for protecting WSNs against attacks. Intrusion detection systems are considered as the second defense line. If these systems are designed effectively, hence, they can successfully detect destructive activities and help protect and maintain network security.

Intrusion detection is considered to be one of the critical research issues which can have potential functions and uses [13]. The next stage after the detection of intrusion, as the last resort, is to tolerate intrusion which is aimed at stopping the intrusion measures of an enemy at the edge of a network. Preventing intrusion against some attacks is not effective [13]. A simple method for detecting an attack is to search for nodes with abnormal traffic profiles. Shin et al. [14] argued that intrusion detection cannot be effective against many attacks. They suggested that each passive attack such as eavesdropping and intrusion detection cannot be 100% effective.

For protecting WSNs against nodes with malicious and selfish behaviors numerous routing protocols have been recently proposed. However, these routing protocols have focused on primary (initial) encryption and identity acknowledgment mechanisms which are not suitable and appropriate for WSNs. Firstly, many of the encryption algorithms, especially asymmetric encryption processes, need high computation capability and high power consumption. Secondly, most of the encryption and identity acknowledgement mechanisms in routing protocols need a center or centralized management.

In this paper, a trust-aware secure routing method has been proposed for WSNs. At first, after routing, fuzzy logic was used for detecting normal sensors and abnormal (malicious) sensors. The concept of trust was used as a limit for detecting dangers. The three concepts of trust, untrust and distrusts were investigated inside the network. Trust level was measured. Hence, based on this method, malicious behaviors are specified by measuring the trust of nodes and paths. Consequently, the securities of the nodes and paths are enhanced. The results of the evaluations indicated that the proposed method can pinpoint and locate malicious nodes. Optimal path between nodes is produced by using MDS-MAP method. In this study, fuzzy logic was usefully used for figuring out the security and treatability of a given network. Abnormal and unnatural sensors are regarded as an internal attack. Trust management schemes have high ability for detecting available malicious nodes and they can make predictions about future behaviors. Hence, they are considered to be a security tool for secure routing.

The rest of the paper is organized as follows: Sect. 1 gives an introduction to security and trust in WSNs. Section 2 briefly reviews the related studies. Section 3 describes the proposed method. Section 4 describe energy consumption model for the proposed scheme. Section 5 indicates the performance evaluation of the proposed scheme. Section 6 gives the conclusion, suggestions for further research and the final remarks of the study.

2 Related Works

In general, all the trust models in WSNs can be divided into two types: central model and distributed models. In central trust models, the base station or a specific trustable interface carries out the operation of accumulating and integrating the trust values of sensor nodes. However, in distributed trust models, sensor nodes themselves accumulate the trust values.

In [15], the authors proposed RFSN (reputation-based framework for high integrity sensor networks) which uses watchdog method for creating trust. Two significant parts of this model are watchdog and reputation system. The surveillance part is responsible for the observation of the behavior of neighboring nodes and distinguishing the behavior of nodes based on cooperation or lack of cooperation. The nodes are classified into two classes of good nodes and bad nodes. The reputation system is responsible for maintaining the reputation of each group. The reputation of a node is determined based on the neighboring nodes' observations of the previous behaviors of that node. Trust in a node indicates the neighboring nodes' belief in the upcoming behaviors of that node [16].

In [17], the authors used the fuzzy logic to introduce the trust calculation method by for WSNs. This method uses reputation values of nodes for measuring the reputation values of paths. Then, the path with the highest reputation value is selected for transmitting packets. The trust model based on the fuzzy logic is deemed to be one of the central models; it should be noted that central models have high energy consumption [17]. One of the merits of using fuzzy reasoning is that it is appropriate for systems which are highly complex and their behaviors cannot be easily figured out. The major problem of this method is its high energy consumption.

In Parameterized and Localized trust management Scheme for sensor networks security (PLUS) model [18], for estimating the degree of trust of one node, each node considers not only its own view about the records of that node but also the neighboring nodes' views about it. For accomplishing this process, nodes play three distinct roles: initiator node, target node and advisory node. One advantage of PLUS method is that all the established communications for estimating the reputation value of nodes are of the single-hop type. Moreover, the reputation values of nodes are not updated periodically; rather, updating is done by changing the reputation values of the target node which results in the overhead reduction of this method. On the other hand, one shortcoming of this method is the addition of HSN packets to controlling packets which not only increases the size of packets but also increases the required energy consumption for transmitting and receiving data. Another problem of this method is that it is not appropriate for WSNs with high traffic since a simpler method is needed for detecting malicious nodes.

In [12], the authors proposed TC-BAC, an access control model for WSNs which is based on the degree of trust and centrality. In this method, the concept of direct and indirect trust is used. Also, in this method, the sensor networks distributed within range are first examined. In [8], the authors presented TARF, a trust model which considers different parameters such as average energy consumption, throughput, PDR, and delay. In this model, each node keeps one neighborhood table which includes the cost level of energy and the trust level of the neighbors. In this method, the neighborhood table is sometimes updated and the redundant cases are eliminated. For maintaining the neighborhood table with the trust level values and energy level for the recognized neighbors, the two components of energy watcher and trust manager are executed which are responsible for registering these values in the table. Each node selects another node with another hop based on the neighborhood table and broadcasts the energy cost to

its neighbors. CORE (Collaborative Reputation) [19] and ATRM (Agent based Trust management) [20] are two other trust models which have been developed for WSNs. In the neural network method which was formerly used for detecting intrusion and preventing attacks, using analytical redundancy and a knowledge-based system, this method was designed in base stations. A sensor node is judged to be destructive in case it tries to feed false information into the sensor networks [21]. In [22], the authors proposed a method in which the complexities of intrusion detection is reduced through a genetic algorithm and the lifespan of these networks is enhanced [22]. In [23], the authors categorized the solutions of creating security in WSNs into three classes: key management, authentication and secure routing and secure services. They found that these methods are suitable for weak attacks. Due to energy consumption limitation in WSNs, intrusion detection system is used for detecting strong attacks so that once an attack is detected, the required warning can be given by the intrusion detection system and the appropriate measures can be taken to prevent the attack. Securing Ad hoc On demand Distance Vector (SAODV) [24] is a secure routing protocol based on initial encryption which can oppose against some routing attacks so as to guarantee the integrity and acknowledgement of identity. All the routing messages in this protocol are illustrated in the digital form and when the PREP message should be indicated by the destination node, intermediate nodes cannot send the message. In [25], the authors developed the A-SAODV protocol for reducing the negative impacts of SAODV. In this protocol, the source node can detect whether or not it should use a single-signature or double signature for the threshold of the load status. Indeed, SAODV and A-SAODV are ad-hoc routing protocols; hence, they are not appropriate for WSNS since these networks have resource limitations. In [26], the authors presented a fuzzy-based trust estimation scheme, T-XLM, a trust-based cross-layering framework to provide minimal defense against security attacks. The proposed scheme is used to formulate imprecise empirical knowledge to ensure secure forwarding of data. Also, they proposed TruFiX, a T-XLM inspired protocol which utilizes multiple parameters pulled through inter-layer information exchange to mitigate the effects of security threats. In [27], the authors proposed an Energy-aware Secure Routing with Trust (ESRT) scheme that maintains a trusted environment, isolate misbehaving nodes and has low control overhead. ESRT considers many parameters for packet routing such as trust, energy, and hop counts.

Building trust is a recent concern in many fields such as web-based services, e-commerce, peer-to-peer networks and WSNs. In WSNs, different methods, technologies and mechanisms for building trust such as fuzzy logic, probabilistic and deterministic methods have been proposed [28–32]. Trust and reputation methods are significant tools which can be used in many areas such as social, economic and computer science fields. Trust systems are appropriate methods for detecting the threats of deceitful or endangered members of a network. These systems fulfill their functions by detecting and identifying malicious nodes and eliminating them from the network [23]. Using a distributed scoring method, power trust system alternatively selects a number of trustable nodes with the highest energy as the energy nodes. In this trust model, at first, a trust coverage network is produced based on the nodes forming the network. When a transaction occurs between a pair of nodes, all the nodes evaluate one another. Hence, nodes alternatively transmit local trust values among each other and are alternatively selected [33]. In peer trust system, the trustability of a node is defined by evaluating that node according to its ability it had for providing services for other nodes in the past. This model reflects the trust values of other available nodes of the society based on their past experiences about the respective node [34].

Table 1 Comparison of the trust models

Trust models	Model architecture	Advantages	Disadvantages
RFSN [16]	Distributed	The first distributed trust model in WSNs	Not registering all the behaviors of nodes
Fuzzy logic-based trust model [17]	Centralized	High speed	High energy consumption
PLUS model [18]	Distributed	Updating trust values by changing the trust value of the destination node	Much overhead due to HSN packets
TC-BAC [12]	Distributed	Using the concept of centrality degree	High consumption of energy and consumption of much time for calculating direct node trust
TARF [8]	Distributed	Functioning well against black hole attacks and message change	It needs more cost and memory for observing neighbors and a poor detection of network problems by using evaluation criteria

Table 1 compares the studied trust models.

3 The Proposed Method

For routing in the proposed method, MDS-MAP algorithm was used to determine optimal path with less errors and the trust model was determined by using fuzzy logic. The method was used in this study is MDS-MAP. The justification for selecting this method is that it is based on distance and has fewer errors for locating optimal path. Also, this method makes use of geometry science and converts the matrix of distance into the matrix of points. The accuracy of this method is higher than those of other methods since it is based on distance. One of the challenges of this method is in converting local maps to global maps.

The proposed scheme includes four-stage model: (1) Measuring the distances of the two nodes from one another. R matrix has the elements of r_{ij} where r_{ij} refers to the distance between the i and the j node or zero in case any distance is not found. (2) Using Dijkestra algorithm for finding the shortest distance between the two nodes. (3) Executing MDS algorithm and finding the location of nodes. (4) Converting local maps to global maps. In the fourth stage, location information of the reference nodes was used and through geometrical conversions such as rotation and displacement, the absolute location of each node was obtained. Such nodes are referred to as reference nodes. The proposed method uses trigonometric and linear algebra principles for computing the relative coordinates of the points based on their two-sided distance. Accurate and effective positioning and locating algorithms are usually considered based on multi-dimensional scale (MDS) in a hierarchical network. Positioning algorithms need guiding nodes which are aware of their own positions so that sensor nodes can specify their own positions. MDS-MAP algorithm is regarded as one of these algorithms which uses MDSs for computing the coordinates of all the nodes based on the relative distance between nodes.

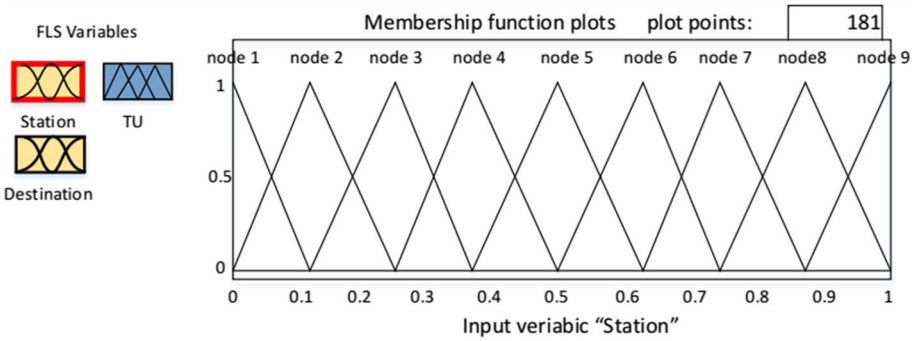


Fig. 1 Membership functions of station input with 9 hypothetical nodes

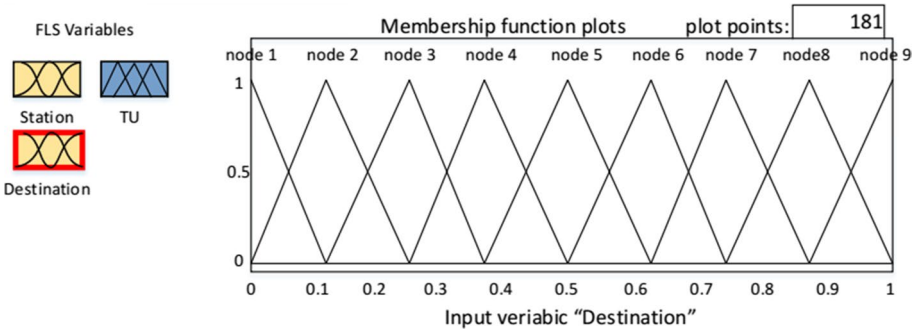


Fig. 2 Membership functions of destination input with 9 hypothetical nodes

Using MDS, distance and G graph with the coordinates of (V, E, P), MDS-MAP algorithm estimates X sensor node and determines its position. At first, the shortest path is measured and in D_{ij} matrix, the shortest path is squared. In the next stage, MDS was used in the D_{ij} matrix for determining the position of X. Hence, in the MDS-MAP algorithm, by specifying the shortest path between the two nodes, the positions of the sensor nodes was determined. That is, if there are two nodes i and j, the shortest path between these two nodes in the $G(V, E, P)$ graph define as a path between them. In Eq. (1), $d_{i,j}$ refers to the shortest path between nodes i and j.

$$D_{ij} = \begin{cases} 0, & i = j \\ d_{ij}^2, & otherwise \end{cases} \tag{1}$$

Indeed, by calculating the coordinate and matrix distances, MDS-MAP algorithm estimates the distances between sensor nodes. In the proposed method, fuzzy logic was used for computing trust as shown in Figs. 1 and 2.

Fuzzy logic has three stages:

i. *Fuzzy adjustment* in this stage, the adjustment degree for the main stages is measured and conditions of fuzzy rules are considered as shown in Figs. 3 and 4.
ii. *Conclusion* a rule conclusion is computed based on the adjustment degree.
iii. *Combination* the transmitted conclusion is converted into a global.

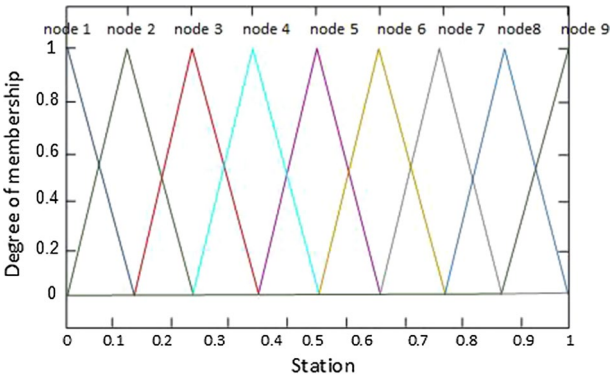


Fig. 3 Membership degree for the trust model

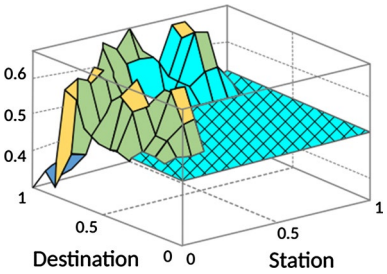


Fig. 4 Graphical schema of the levels

Using fuzzy logic in WSNs is highly useful for detecting normal and unnatural sensors. By attacking the network, unnatural sensors can pollute it. In this method, the three concepts of trust, lack of trust and rejecting all the trusts within the network were introduced. For using a secure and safe WSN, the degree between sensor nodes should be calculated. For measuring trust level for the sensor node, T is defined as trust and U is defined as non-trustable.

$$T = \frac{avg(T_i, T_j)}{1 - \left(avg(T_i, U_j) + avg(T_j, U_i)\right)} \tag{2}$$

$$U = \frac{avg(U_i, U_j)}{1 - \left(avg(T_i, U_j) + avg(T_j, U_i)\right)} \quad 0 \le T \le 1, \quad 0 \le U \le 1$$

where in Eq. (2), i, j are from the set of sensor nodes. Using this method, the evaluated value for a path is obtained through Eq. 3:

$$Evaluation\_value = \frac{T}{T + U} \tag{3}$$

Using MDS-MAP method, we generate a trustable and optimal path between the nodes. Fuzzy logic was used to indicate how trust mechanisms are effective in our routing method and selecting a path from the source node to the destination node. Indeed, it can be argued that fuzzy logic is a reliable and trustable method for establishing secure communications within WSNs. Through fuzzy logic, an attempt was made to figure out the secureness or

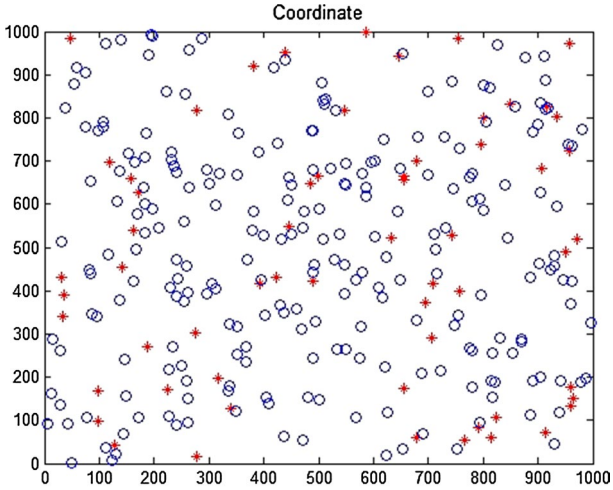


Fig. 5 Distribution of nodes

trust for a WSN. In this study, fuzzy logic was used to distinguish normal sensors from unnatural sensors. Unnatural sensors can be regarded as internal attacks or in case such nodes are controlled by intrusive users, all the WSN structure will be polluted. Trust refers to a set of sensor assembly and aggregation which investigates the interactions among sensors in the network in earlier times and based on it, decision making is done. Fuzzy logic has two inputs, i.e. source and destination and a TU output, T is for the trust rate and U is for the rate of untrust. The operation conducted in this method is that a number of nodes have been placed in this station and they are membership functions of station input. Initiating routing requires the placement of the nodes (Fig. 5). After determine network topology, the neighboring degree of the nodes is specified. After obtaining the optimal path with the aid of the closest neighbor of the node, for preserving location, the initial energy and power of the network is sent back to the defined topology. MDS-MAP algorithm was used for determining the optimal path with fewer errors and also the Regular model was used in this study. Maximum location errors are randomly diffused by the reference nodes. All the conditions for using MDS-MAP method on all the nodes and reference nodes were considered. The distance of the shortest path was calculated by using the signal reception power of the neighboring node. Euclidean distance between two nodes, i.e. *Xi* and *Xj* is obtained in an m-dimensional space through Eq. 4:

$$X_i = \left(X_{i1}, X_{i2}, \ldots, X_{im}\right)$$

$$X_j = \left(X_{j1}, X_{j2}, \ldots, X_{jm}\right)$$

$$d_{ij} = \sqrt{\sum_{k=1}^{m} \left(x_{ik} - x_{jk}\right)^2} \tag{4}$$

$$I(P) = D + E \tag{5}$$

where p denotes the transmission center and X coordinate can be computed through two axes for singular value decomposition (SVD). For P, $n \times n$ matrix for the n point and m dimensions of each point, we have Eq. (6):

$$\sum_{k=1}^{m} x_{ik} x_{jk} = -\frac{1}{2}\left(p_{ij}^2 - \frac{1}{n}\sum_{j=1}^{n} p_{ij}^2 - \frac{1}{n}\sum_{i=1}^{n} p_{ij}^2 + \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^2 \right) \tag{6}$$

Since errors have no effect on it and channels and paths are active, regular model was used in this study. There are numerous paths from the source node to the destination node. Using the fuzzy logic, the trust model selects an appropriate path from the source to the destination so that a safe and secure communications can be maintained. After using the information of the computed results, each node decides on whether to establish communications or not. Trust information should not increase through diffusing and the destination nodes is assumed to be a trusted entity in the trust management system. In general, routing should be accomplished in a way that less energy is consumed and at the same time, security and trust should be taken into consideration. When a node inside a path wants to transmit a packet to another node, it finds an optimal path for transmitting the packet. At first, it tries to select short paths with less errors. Indeed, by computing the trust values of the paths leading to the destination node, the node selects paths with higher trust values and checks whether there are unnatural and abnormal sensors in the selected path. At first, sensor nodes are homogenous. That is to say, they have identical processing power, communication power and energy resources. Consequently, the structure of the routing in the network will be more effective. Hence, the transmissions from the source to the destination will be easier and less time will be needed for finding the trust path. Also, natural nodes will be easily distinguished from unnatural nodes and less energy will be consumed.

4 Energy Consumption Model

The required energy consumption model for the communication among sensor nodes is defined according to Eq. (7). The amount of energy consumption for transmitting a message from one sensor to another sensor with the distance of d is equal to $E_{TX}(k, d)$.

$$E_{TX}(k,d) = \begin{cases} E_{elec} \times k + E_{fs} \times k \times d^2 & (d < d_0) \\ E_{elec} \times k + E_{mp} \times k \times d^4 & (d \geq d_0) \end{cases} \tag{7}$$

In Eq. (7), E_{elec} refers to the basic energy which is required for executing transmitting or receiving circuits. This energy is consumed in the electronic circuit of the receiver or transmitter for receiving or transmitting a bit of data packet. Parameter K refers to the number of transmitted packets; Parameters E_{fs} and E_{mp} indicate the required energy for supporting transmission. The value of d_0 is obtained through Eq. (8).

$$d_0 = \sqrt{E_{fs}/E_{mp}} \tag{8}$$

For receiving k data bits, a radio model is defined according to Eq. (8). The amount of energy consumption for receiving k data bits is equal to $E_{RX}(k)$. In Eq. (9), it is assumed that each sensor node receives only one data packet from its neighboring nodes.

$$E_{RX}(k) = E_{elec} \times k \tag{9}$$

Table 2 Simulation parameters

Parameter	Value
Number of nodes	300
Number of reference nodes	60
Shared channel	200 m
Used model	Regular
Estimated time	20 ms
The initial path	200 m
Network size	1000 m × 1000 m
Initial energy	0.5 j
E_{elec}	50 nj/bit
E_{fs}	10 pj/bit/m^2
E_{amp}	0.0013 pj/bit/m^4
d_0	87 m
Position of the sink	(0,0)
Radio range of each node	60 m

5 Performance Evaluation

We used a simulation approach to evaluate the performance of our protocol. The simulation was implemented using Matlab software. Sensor nodes randomly distributed in the simulation environment and multi-hop transmissions was used between source and destination nodes. MDS-MAP algorithm with the aid of the nearest neighbor was used for determining the optimal path. Table 2 shows simulation parameters values.

After the shortest path with fewer errors is found, by calculating the trust values of the paths via fuzzy logic, we can find the trustable paths from the source node to the destination node. Up to this stage, fuzzy logic was used in the proposed method for going through the path and for secure transmitting the packets to the destination node. Hence, network nodes are trustable. In case the network node has high trust value, other nodes of the network can trust it; hence, they can safely transmit nodes to it and receive nodes from it. When a source node wants to transmit packets to a destination node through multi-hop communications, it examines the trust values of the paths and selects the path with the highest trust value. The proposed method distributes nodes randomly and the communication between nodes is established (Fig. 5).

$$\text{Source} = [49\,4\,39\,42\,20\,4\,5\,18\,26\,39\,42\,32\,47]$$
$$\text{Target} = [5\,45\,22\,1\,8\,28\,26\,8\,13\,33\,36\,39\,20]$$

5.1 The Amount of Spent Time

As the time passes, the network proceeds normally and the trustable path is gone through by considering the distance (high trust and low distance). However, as an attack exist in the network, the spent time in the network increases. When there is a trustable path from the source node to the designation node, messages go through the safe and trustable path; consequently, it will take less time. Figure 6 illustrates the time spent for executing the proposed method.

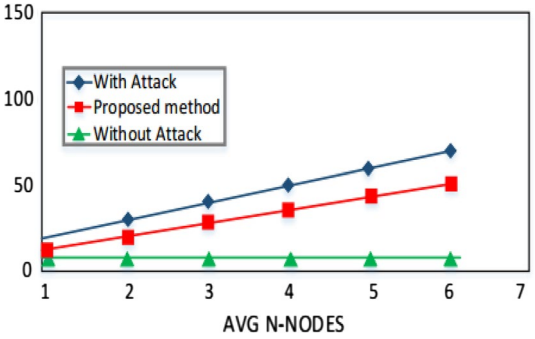


Fig. 6 Time spent in the network with and without attack

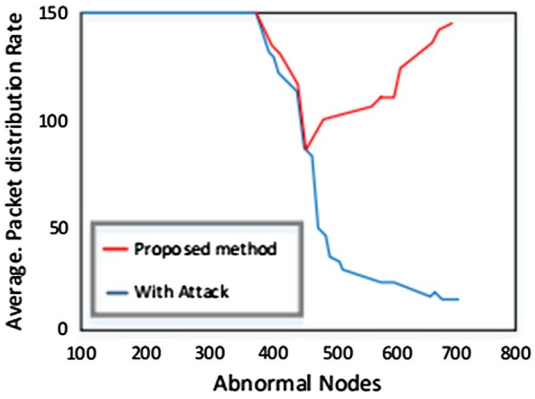


Fig. 7 The impact of attack on average packet distribution rate

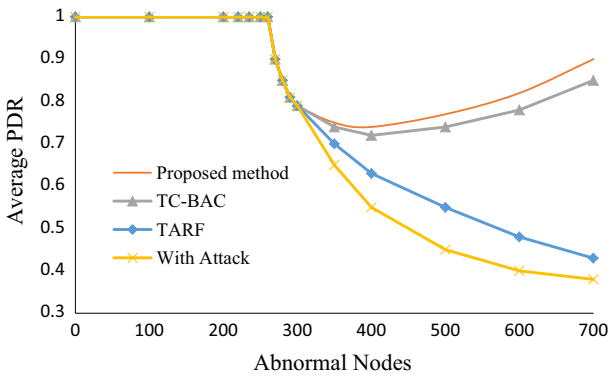


Fig. 8 Average packet delivery rate

5.2 Average Packet Delivery Rate

When an attack is recognized in the network, the average packet distribution rate decreases. When there is no attack in the network, the average packet distribution rate comes close to 100%. Figure 7 illustrates that as attack in the network increases, packet distribution decreases. The proposed method helps source nodes to detect an attack faster and goes

through trustable paths so that packets can be safely delivered to the destination. It also helps source nodes to better resist against attacks.

As shown in Fig. 8, when there is no attack in the network, the average packet delivery rate comes close to 100%. However, in the presence of attack, packet delivery rate significantly decreases.

5.3 Security Model

In general, it can be maintained that WSNs are vulnerable to attacks. In the proposed method and the two above-mentioned methods, it assumes that all the usual sensor nodes have compromised. In contrast with average sensor nodes, the sink node has high capability for dealing with common attacks since it has a more complex hardware. In the TC-BAC method, both direct and indirect trusts have been used (direct trust is based on the direct observations of the node which has participated in data exchanges and indirect trust is based on trust among distributed nodes). In TARF [8], an optimal method was selected based on trust, energy consumption and trustability. The amounts of the trusts of paths were calculated according to the neighborhood table where trust values are considered within them. Nevertheless, in the method proposed in this study, trust is considered to be a set of past interactions among sensors.

In the proposed method, at first, it assumes that all the sensors have compromised. However, in TC-BAC method, there are two types of nodes, i.e. well-behaved and badly-behaved nodes and the two types of Selfish and Dos attacks have been investigated in this method. In TC-BAC, attacks are investigated for examining network flooding via unwanted traffic. By evaluating the degree of trust of neighbors within the routing table in the TARF [8] method, the path with efficient energy is selected. In this method, the node N decides on which path it should use so that data packet can reach the base station. In contrast, fuzzy logic is used in the trust model of the proposed method. One of the advantages of using fuzzy logic is that a fast but approximate method is preferred. Another merit of using fuzzy logic is that it can examine highly complex systems and figure out their behavior.

In the proposed method, source and destination nodes were selected. Then, the suggested calculation methods were implemented on the path and the degree of trust for the paths are measured. Then, the packets were transmitted through the paths with the highest reputation. The proposed method uses the trust value of the nodes for measuring the trust values of the paths. Then, as mentioned above, the path with the highest trust was selected for transmitting packets. Fuzzy logic can be used for giving values to indeterminate values and inaccurate data. Hence, the method proposed in this paper can be used for selecting the proper route from the source to the destination node. It should be noticed that all the three methods have high energy consumptions. However, inasmuch as the proposed method uses a short and trustable path, it can reduce the delay related to finding a new path. The energy consumption of the proposed method is less than those of TC-BAC and TARF [8]. Measuring the trust of direct node in the TC-BAC method is considerably time-consuming. Also, in the TARF method, seeking a path with high trust and low energy consumption in the table is time-consuming. In contrast, the proposed method significant uses less time than the TC-BAC and TARF methods since it uses the shortest path by considering security, trust and employing fuzzy logic.

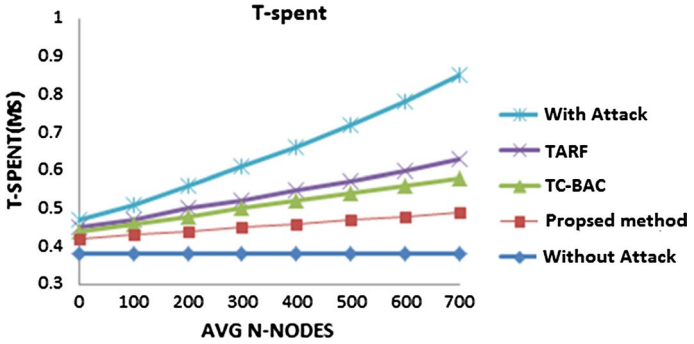
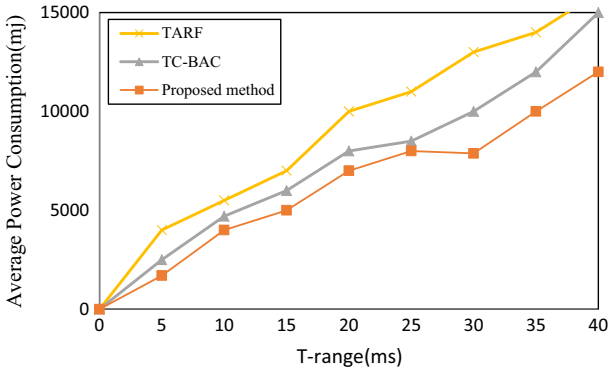


Fig. 9 Average elapsed time

Fig. 10 Average power consumption



5.4 Average Elapsed Time

As shown in Fig. 9, when there is no attack in the network, network functions properly but when an attack occurs in the network, the number of nodes increases which will lead to an increase in the elapsed time. Indeed, network is highly vulnerable to attack since more time will be required to find safe paths for the transmission of packets. It can be argued that the attack detection speed is high in the proposed method due to using routing protocol and fuzzy logic.

5.5 Power Consumption

As it can be observed from Fig. 10, power consumption in the proposed method is less than those of TC-BAC and TARF [8] methods. Indeed, as discussed earlier in the paper, the proposed method uses optimal paths with short distances. Furthermore, the proposed method acts faster than them in detecting attacks since it has the identity number of the source node's neighbor. Consequently, energy consumption is significantly reduced in the proposed method. In contrast, TC-BAC method needs more calculations for doing the same task which leads to the consumption of more energy. Moreover, in the TARF method, finding an optimal path from the neighborhood table and updating the table for removing repeated records results in the consumption of more energy.

6 Conclusion

In this paper, a routing protocol was proposed for optimizing security and trust in WSNs. Different types of trust and attack were examined in this study and a new method was introduced for enhancing security and trust in WSNs. The method proposed in this paper was aimed at reducing energy consumption and, hence, enhancing network lifetime. The proposed method was compared with TC-BAC and TARF [8]. The results of simulations indicated that the proposed method functions better than both TC-BAC and TARF [8] in terms of the following parameters: packet delivery rate, average elapsed time and energy consumption. In future studies, the scheme will be improved through the implementation of an evaluation strategy for further intrusion and attacks detection.

References

1. Nikokheslat, H. D., & Ghaffari, A. (2017). Protocol for controlling congestion in wireless sensor networks. *Wireless Personal Communications, 95*(3), 3233–3251.
2. Ghaffari, A. (2015). Congestion control mechanisms in wireless sensor networks: A survey. *Journal of Network and Computer Applications, 52,* 101–115.
3. Wu, F., Xu, L., Kumari, S., & Li, X. (2017). A new and secure authentication scheme for wireless sensor networks with formal proof. *Peer-to-Peer Networking and Applications, 10*(1), 16–30.
4. Zhou, Y., Fang, Y., & Zhang, Y. (2008). Securing wireless sensor networks: A survey. *IEEE Communications Surveys Tutorials&, 10*(3), 6–28.
5. Djenouri, D., Khelladi, L., & Badache, N. (2005). A survey of security issues in mobile ad hoc networks. *IEEE Communications Surveys, 7*(4), 2–28.
6. Ahmed, A., Bakar, K. A., Channa, M. I., Khan, A. W., & Haseeb, K. (2017). Energy-aware and secure routing with trust for disaster response wireless sensor network. *Peer-to-Peer Networking and Applications, 10*(1), 216–237.
7. Jin, X., Liang, J., Tong, W., Lu, L., & Li, Z. (2017). Multi-agent trust-based intrusion detection scheme for wireless sensor networks. *Computers and Electrical Engineering, 59,* 262–273.
8. Zhan, G., Shi, W., & Deng, J. (2012). Design and implementation of TARF: A trust-aware routing framework for WSNs. *IEEE Transactions on Dependable and Secure Computing, 9*(2), 184–197.
9. Pirzada, A. A., McDonald, C., & Datta, A. (2006). Performance comparison of trust-based reactive routing protocols. *IEEE Transactions on Mobile Computing, 5*(6), 695–710.
10. Li, X., Jia, Z., Zhang, P., Zhang, R., & Wang, H. (2010). Trust-based on-demand multipath routing in mobile ad hoc networks. *IET Information Security, 4*(4), 212–232.
11. Cho, J.-H., Swami, A., & Chen, I.-R. (2011). A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys and Tutorials, 13*(4), 562–583.
12. Duan, J., Gao, D., Heng Foh, C., & Zhang, H. (2013). TC-BAC A trust and centrality degree based access control model in wireless sensor networks. *Ad Hoc Networks, 11*(8), 2675–2692.
13. Mitchel, R., & Mitchel, I.-R. (2014). A survey of intrusion detection in wireless network applications. *Computer Communications, 42,* 1–23.
14. Shin, S., Kwon, T., Jo, G.-Y., Park, Y., & Rhy, H. (2010). An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. *IEEE Transactions on Industrial Informatics, 6*(4), 744–757.
15. Ganeriwal, S., & Srivastava, M. (2004). Reputation-based framework for high integrity sensor networks. In *Proceedings of the ACM workshop on security of ad hoc and sensor networks* (pp. 66–77).
16. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. (2013). Management and applications of trust in wireless sensor networks: A survey. *Journal of Computer and System Sciences, 8*(3), 602–617.
17. Kim, T. K., & Seo, H. S. (2008). A trust model using fuzzy logic in wireless sensor network. *Proceedings of World Academy of Science Engineering and Technology, 18,* 63–66.
18. Yao, Z., Kim, D., & Doh, Y. (2008). PLUS: Parameterized and Localized trust management Scheme for sensor networks security. In *IEEE international conference on mobile ad-hoc and sensor systems* (pp. 437–446).
19. Michiardi, P., & Molva, R. (2002). CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks. In *The IFIP TC6/TC11 sixth joint working conference on*

communications and multimedia security: Advanced communications and multimedia security Portoroz, Slovenia (pp. 107–121).
20. Boukerch, A., Xu, L., & El-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications*, 30(11–12), 2413–2427.
21. Mishra, A., Sudan, K., & Soliman, H. (2010). Detecting border intrusion using wireless sensor network and artificial neural network. *In 2010 6th IEEE international conference on distributed computing in sensor systems workshops (DCOSSW)* (pp. 1–6).
22. Khanna, R., Liu, H., & Chen, H.-H. (2009). Reduced complexity intrusion detection in sensor networks using genetic algorithm. In *IEEE ICC*.
23. Xiong, L., & Liu, L. (2004). Peer trust: supporting reputation-based trust in peer-to-peer communities. *IEEE Transactions on Knowledge and Data Engineering, 16*(7), 843–857.
24. Zapata, M. G., & Asokan, N. (2002). Securing ad hoc routing protocols. In *Proceedings of the 1st ACM workshop on wireless security* (pp. 1–10).
25. Cerri, D., & Ghioni, A. (2008). Securing AODV: The A-SAODV secure routing prototype. *IEEE Communications Magazine, 46*(2), 120–125.
26. Umar, I. A., Hanapi, Z. M., Sali, A., & Zulkarnain, Z. A. (2017). TruFiX: A configurable trust-based cross-layer protocol for wireless sensor networks. *IEEE Access, 5,* 2550–2562.
27. Ahmed, A., Bakar, K. A., Channa, M. I., Khan, A. W., & Haseeb, K. (2017). Energy-aware and secure routing with trust for disaster response wireless sensor network. *Peer-to-Peer Networking and Applications, 10*(1), 216–237.
28. Vasserman, E. Y., & Hopper, N. J. (2013). Vampire attacks: Draining life from wireless ad hoc sensor networks. *IEEE Transactions on Mobile Computing, 12*(2), 318–332.
29. Daojing, H., Chun, C., Chan, S., Bu, J., & Vasilakos, A. V. (2012). ReTrust: Attack-resistant and lightweight trust management for medical sensor networks. *IEEE Transactions on Information Technology in Biomedicine, 16,* 623–632.
30. Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). Active Trust: secure and trustable routing in wireless sensor networks. *IEEE Transactions on Information Forensics and Security, 11*(9), 2013–2027.
31. Yu, Y., Li, K., Zhou, W., & Li, P. (2012). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications, 35*(3), 867–880.
32. Ayday, E., & Fekri, F. (2012). An iterative algorithm for trust management and adversary detection for delay-tolerant networks. *IEEE Transactions on Mobile Computing, 11*(9), 1514–1531.
33. Kamvar, S., Schlosser, M., & Garcia-Molina, H. (2003). The EigenTrust algorithm for reputation management in P2P networks. In *Proceedings of the international world wide web networks, Proceedings of the international world wide web conference* (pp. 173–186).
34. Zhoh, R., & Hwang, K. (2007). PowerTrust: A robust and scalable reputation system for trusted peer to peer computing. *IEEE Transaction on Parallel and Distributed Systems, 18*(4), 460–473.

Azam Beheshtiasl received his BSc and MSc degrees in computer engineering from the institute of Daneshvaran and Islamic Azad University (Tabriz branch), TABRIZ, IRAN in 2009 and 2017 respectively. Her research interests are mainly in the field of Wireless Sensor Networks (WSNs), Mobile Ad Hoc Networks (MANETs) and networks security.

Ali Ghaffari received his B.Sc., M.Sc. and Ph.D. degrees in computer engineering from the University of Tehran and IAUT (Islamic Azad University), TEHRAN, IRAN in 1994, 2002 and 2011 respectively. As an assistant professor of computer engineering at Islamic Azad University, Tabriz branch, IRAN, his research interests are mainly in the field of software defined network (SDN), Wireless Sensor Networks (WSNs), Mobile Ad Hoc Networks (MANETs),Vehicular Ad Hoc Networks (VANETs), networks security and Quality of Service (QoS). He has published more than 60 international conference and reviewed journal papers.