IntelligentAutomationAndSoftComputing,2020
Copyright © 2020, TSI® Press
Vol.26,no.2, 217–226
https://doi.org/10.31209/2018.100000064

# Hybrid Soft Computing Technique Based Trust Evaluation Protocol for Wireless Sensor Networks

**Supreet Kaur, Dr. Vijay Kumar Joshi**

Department of Computer Science and Engineering, IKG Punjab Technical University, Jalandhar, Punjab, India

**ABSTRACT**

Wireless sensor networks (WSNs) are susceptible to safety threats due to cumulative dependence upon transmission, computing, and control mechanisms. Therefore, securing the end-to-end communication becomes a major area of research in WSNs. A majority of existing protocols are based upon signature and recommended-based trust evaluation techniques only. However, these techniques are vulnerable to wormhole attacks that happen due to lesser synchronization between the sensor nodes. Therefore, to handle this problem, a novel hybrid crossover-based ant colony optimization-based routing protocol is proposed. An integrated modified signature and recommendation-based trust evaluation protocol for WSNs is presented. Extensive experiments reveal that the proposed technique outperforms existing protocols in terms of network lifetime, bandwidth, and execution time.

**KEY WORDS**: Ant colony optimization, Crossover, Energy efficiency, Wireless sensor networks.

## 1 INTRODUCTION

WIRELESS sensor networks (WSNs) are becoming popular day by day due to its wide range of applications. WSNs are extensively utilized in various applications such as ocean floors, barren regions, mountains and battlegrounds Mohanty, et al. (2016). However, WSNs are vulnerable to various attacks such as sinkholes, wormholes, gray holes and black holes Singh, et al. (2016). A large number of sensors might be placed within a particular area, and their movement is frequently observed and supervised by a reliable and trusted unit, usually called a sink or base station (BS) Mohanty, et al. (2013).

To prevent various security attacks, there is a need to design adequate security protocols Yousefi, et al. (2012). From existing reviews, a wormhole attack is found to be more dangerous in WSNs. In this situation, an attacker obtains data packets at one position in the network, tunnels, and then replaces them at a different remote position in the sensor field Madria, et al. (2009). It can be effortlessly initiated by an attacker without compromising any sensor node. The majority of traditional routing protocols do not have mechanisms to protect the WSNs against wormhole attacks Poovendran, et al. (2007). The path demand can be tunneled to a target sensor field by an attacker using wormholes. Therefore, nodes in the target sensor field construct the path using an attacker. Afterwards, an attacker can alter/corrupt/ drop the data packets Yun, et al. (2007).

A novel wormhole attack detection approach is designed using statistical analysis. In this technique, a sensor node can monitor and track wormhole neighbors using the neighborhoods discovery algorithm. Afterwards, a k-means clustering is utilized to recognize a wormhole attack Tian, et al. (2012). Statistical analyses are also used to monitor a wormhole attack in a multi-path environment Qian et al. (2007). However, Tian, et al. (2012) and Qian et al. (2007) based techniques become unsuccessful when prior information for statistical analysis is not available.

A lightweight countermeasure is designed for wormhole attack depends on overhearing neighbor communication. It allows monitoring of the wormhole attacker which is followed by isolation of the malicious nodes Khalil, et al. (2007). A novel lightweight countermeasure for wormhole attack detection is designed using localized–decentralized algorithm. It assures that no wormhole attack has happened while using connectivity data, as implied by the underlying communication graph Giannetsos, et al. (2014). A secure ad-hoc on-demand distance vector routing protocol was proposed by Su et al. It considers a link-disjoint multi-path during route discovery and

CONTACT Supreet Kaur Oberoisupreet9@gmail.com

provides greater route selections to avoid malicious nodes. However, it uses only one path to transmit data Su, et al. (2010).

A roundtrip time (RTT)-based wormhole attack detection technique is implemented. RTT secures WSNs against a wormhole attack for multi-rate transmissions Qazi, et al. (2013). A centralized method is designed to monitor wormholes. The proposed method guarantees a good lower bound of successful detection rate Ji, et al. (2015). A time-based countermeasure is proposed to avoid the limitations of the existing time-based wormhole attack detection. In this technique, the sensor nodes neither demand synchronized clocks, nor they request to predict the sending time. Therefore, they are capable of fast switching between the receiver and source nodes Khabbazian, et al. (2009).

A wormhole resistant hybrid technique (WRHT) utilized Watchdog and Delphi schemes and ensures that the wormhole cannot be left untreated in WSNs Singh, et al. (2016). Existing researchers have neglected the relationship between the ratio of malicious users and the ratio of anchors in the WSNs, to ensure trustworthiness of the crowd-sensed data Yao, et al. (2017). The impact of the relation between the ratio of malicious users, the ratio of anchors is also ignored Pouryazdan, et al. (2016). The ratio of anchors on the crowd source utility in the presence of anchor nodes in WSNs is also ignored Pouryazdan, et al. (2017). The impact of the relation between the ratio of malicious users and the ratio of anchors on the user utility in the presence of anchor nodes in a WSNs Li, et al. (2017) are also ignored.

The review on existing security protocols of WSNs has shown that the detection of a wormhole attack is still a challenging issue in WSNs Han et al. (2014). Therefore, the existing protocols either demand specialized hardware or make strong assumptions to detect wormhole attacks, which limit the usability of these techniques Hsu et al. (2010). Thus, the existing protocols have poor efficiency in detecting the randomization behavior of attackers.

In this paper, it is found that the techniques are vulnerable to wormhole attacks, which happen due to lesser synchronization among the sensor nodes. Therefore, to handle this problem, an integrated modified signature and recommendation-based trust evaluation protocol for WSNs is proposed. Further enhancements have been done by designing a novel crossover-based ant colony optimization to improve the routing process. The extensive experiments are carried out, which reveal that the proposed technique outperforms other approaches.

The proposed protocol has the following benefits over the existing signature-based protocols: (i) Comparing to the existing protocol, the proposed protocol can be implemented in a faster and more lightweight manner. (ii) The proposed protocol seems to be more efficient than the existing protocols. In the proposed protocol, only the ratings of trustworthy recommenders are considered, because collecting the opinions from reliable recommenders consume a large amount of time and bandwidth resources.

Therefore, the proposed protocol can overcome the issues associated with existing protocols. Thus, the proposed protocol has an ability to detect a wormhole attack in a more efficient way and with good speed. The integration is achieved by introducing a new prototype which will evaluate the confidence values based on rules of these two trust evaluation techniques. Thus, the proposed protocol provides more secure and accurate results than the existing protocols.

## 2 PROPOSED TECHNIQUE

THIS section describes the proposed technique. Initially, the modified-signature-based trust evaluation is described. Then, the recommendation-based trust evaluation is discussed.

### *2.1 Hybrid crossover-based ant colony optimization*

Figure 1 shows step-by-step methodology of the proposed technique. Each step of the proposed technique plays a significant role to detect the wormhole attacker node in WSNs successfully.

**Step 1:** Initially, the sensor nodes are deployed in the sensor field with the help of normal distribution with mean=0 and variance=1. Each node has its own coordinates in the sensor field and initial energy (in joules). The parameters setting for sensor field are done by considering the standard parameters (obtained from Lower energy efficient adaptive clustering hierarchy (LEACH) Protocol) Hussian, et al. (2013).

**Step 2:** Initialize the sensor nodes as ants along with the base station (BS) as a destination.

**Step 3:** In this step, the energy-aware clustering protocol is considered to develop cluster heads from the active sensor nodes. After that, the cluster heads are evaluated using clustering, which is based upon General self-organized tree-based energy-based routing protocol (GSTEB) Zi and Zhong (2015).

**Step 4:** In this step, the nodes which have become cluster heads, communicate their information with the member nodes (i.e., the nodes which have not been selected as a cluster head in given round). In this step, the member nodes are associated with cluster heads Lee et al. (2017).

**Step 5:** In this round, each sensor node associated with its nearest cluster head is based on the Euclidean distance formula. After that, each node sends data to its cluster head in Time division multiplexing access (TDMA) fashion Li and song (2016).

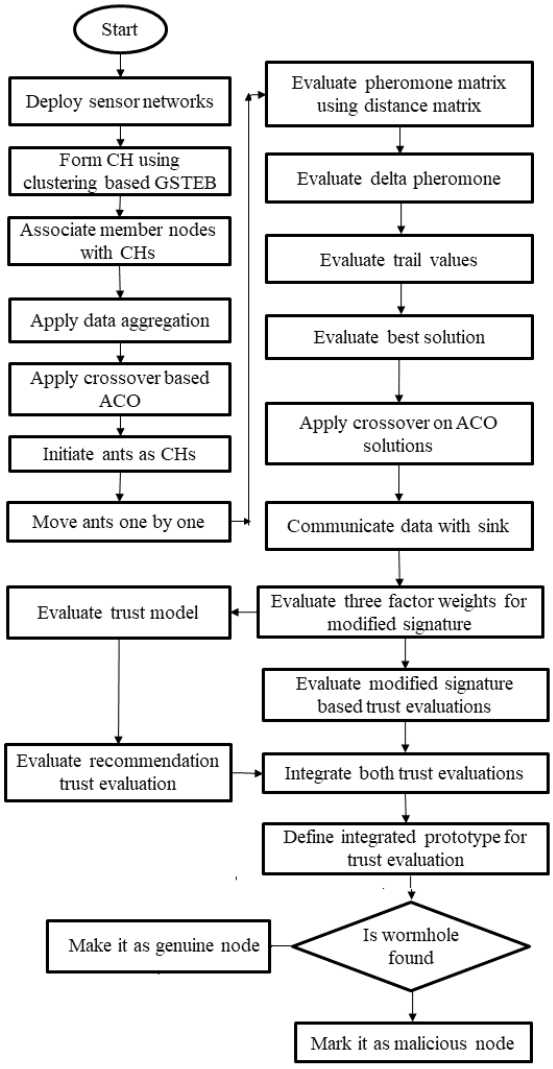


**Figure 1. Flowchart of the proposed secured protocol.**

**Step 6:** In this step, the inter-cluster data aggregation is formed, on the basis of GSTEB and hybrid soft computing technique. The sensor nodes collect sensory information via monitoring the geographical area. Sensory information in the sensor network is then combined, by a sink node, using wireless hop-by-hop broadcast Li, et al. (2017). Data aggregation helps to conserve the energy. It also helps to reduce the total amount of network transfer and energy utilization on sensor nodes Ma, et al. (2011).
**Step 7:** In this step, the cluster heads act as ants and they will move one by one towards their destination.
**Step 8:** In this step, the initial paths will be formed on the basis of pheromone. After that, delta matrix will be evaluated on the basis of distance matrix Sharma, et al. (2016).
**Step 9:** In this step, the delta pheromone is evaluated. Pheromone is a chemical substance which is produced and released into the environment by ants that affect the behaviour of others ants. It attracts following ants so that they will likely search in the same region of the search space Tang Hui, et al. (2011). Delta pheromone (also known as global pheromone) is generated by the whole population and is considered as the best value of population (i.e., the population which is more near to target will get the best value) Wei, et al. (2012).
**Step 10:** After the evaluation of delta pheromone, the trial values are evaluated.
**Step 11:** In this step, the best solution is evaluated on the basis of trial values.
**Step 12:** After the evaluation of best solution, the crossover operator is applied to the solutions obtained from ant colony optimization. In this step, the initial paths have been formed by using pheromones which will be further reduced by using the crossover operator of genetic algorithm and data will be communicated with sink. Crossover is a process of taking more than one parent solution and producing a child solution from them. It combines the characteristics of two solutions (parents) in order to generate a new solution. This operator is inspired in such a way that the genetic code of one individual is inherited by its descendants in nature Zhang, et al. (2017).

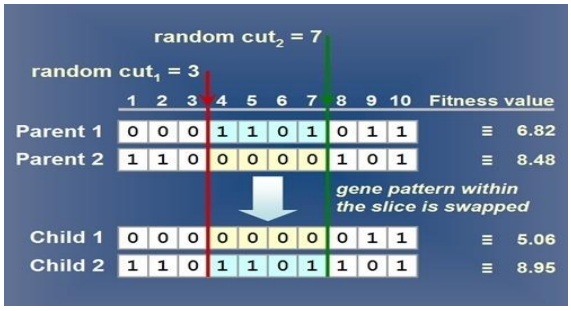


**Figure 2. Crossover analysis.**

The effect of the crossover operator is shown in Figure 2. Here, parent1 and parent 2 are obtained from the ant colony optimization. The random two-point crossover operator is applied on parent 1 and parent 2. The randomly generated points are 3 and 7, respectively. Also, the fitness values of parent 1 and 2 are 6.82 and 8.48, respectively. Two child solutions are developed from these parents who have fitness values of 5.06 and 8.95, respectively. Child 1 has minimum distance as compared to parent 1. Therefore, the best solution is updated by child 1.
**Step 13**: When the crossover operator is applied to the solutions obtained from the ant colony optimization, the completed data will be communicated to the sink node i.e., base station.
**Step 14:** The wormhole attack is applied on the selected path between available cluster heads and the sink. The wormhole continuously drops the packets sent by given sensor nodes. It damages the throughput

of designed protocol a lot. Therefore, we have reduced the security of GSTEB by applying well-known wormhole attack.

**Step 15:** After that, the two things will happen i.e.,

(a) A trust model is evaluated by using three-factor weights for a modified signature. These weight factors are number weight, time delay weight, and context weight.

(b) A number weight is used to balance the robustness against collision and bandwidth consumption.

(c) A time delay weight evaluates the modified signature value with previously available signature value. Therefore, the old modified signatures are unreliable. It is because the behavior of trustee may change from honest to malicious. Therefore, the delay in delivery of a packet is considered to be unreliable.

(d) A context weight evaluates the behavior of a node with respect to its radius. A node showing more radius has more probability to be a malicious node.

**Step 16:** In this step, the modified signature is evaluated. This evaluation is done on the basis of two factors i.e.

(a) An evaluation based on recommendations identifies all trustworthy recommenders and presents the details of the recommendation-based trust calculation method. Owing to the sparse and highly dynamic characteristic, there is no sufficient or long-term trust which introduces the idea of allowing nodes to send several testing requirements (to which the senders have known the similar solutions in advance) for each other. Thus, it calculates the trust value of receivers according to the accuracy and timelines of responses.

(b) An evaluation based on the signature certifier generates a modified signature and then it is sent to the trustee. When the trustee needs to release a message, it first chooses the most advantageous modified signatures from its local storage. It can be conducted in a more fast and lightweight manner while it is more vulnerable to the collision as the certifiers are strange to the trustor in most cases.

**Step 17:** In this step, both trust evaluations are integrated in order to achieve the more accurate evaluation result.

**Step 18:** In this step, the integrated prototype for the trust evaluation is defined to check the existence of wormhole. If there exists a wormhole, mark it as a malicious node; otherwise, mark it as a genuine node.

The following section describes the various steps which are required to select the communication path using the hybrid soft computing approach.

1. Initialize the sensor nodes as ants along with the Base station (BS) as a destination.
2. Moving of virtual ant depends on the amount of pheromone on the BSs distances.
3. The first step in ant colony optimization is the trail selection between neighboring clusters. A set of artificial ants (NSs) are simulated from the NSs to the BS. The forward ants select the next BS randomly for the first time taking the information from the distance matrix. The ants who are successful in reaching the BS, update the pheromone deposit at the edges visited by them by an amount (i.e., CL), where L is the total path length of the ant and C is a constant value that is adjusted according to the experimental conditions to the optimum value.
4. The next set of ants learn from the pheromone deposit feedback left by the previously visited ants and will be guided to follow the shortest path.
5. When an individual ant walks from NSi to NSj, the probability in the selection rule for a single ant is calculated as follows:

$$P_{i,j} = \frac{(\tau_{i,j})^{\alpha} + (\eta_{i,j})^{\beta}}{\Sigma(\tau_{i,j})^{\alpha}(\eta_{i,j})^{\beta}} \quad (1)$$

Here, $\tau_{i,j}$ represents the amount of pheromone deposit from cluster head(CHi) to cluster head (CHj). $\eta_{i,j}$ is the trail visibility function that is equivalent to the reciprocal of the energy distance between CHi and CHj. $\alpha$ is the parameter to adjust the amount of pheromone $\tau_{i,j}$. $\beta$ is a parameter to adjust the heuristic visibility function $\eta_{i,j}$.

6. If the link between two NSs exists, then
   $P_{i,j}$ will be updated
   else
   $P_{i,j} = 0$.
   end
7. Evaluate the distance between the CHi and CHj as:

$$\eta_{i,j} = \frac{1}{E_{DIS(i,j)}}$$

$$E_{DIS}(i,j) = \left(E_{TR_{ELE}} + \gamma \times \| d_{i,j} \| 2^{\lambda}\right) \times S \quad (2)$$

Here, $E_{DIS}(i,j)$ represents the energy distance metric between two Cluster heads i and j. $d_{i,j}$ represents the Euclidean distance. $E_{TR\_ELE}$ is the transmission energy and $\gamma$ is a coefficient of amplifying and S is the pack size.

8. P values will be updated by those ants which have reached the BS successfully.
9. Pheromone evaporation ($\rho$) on the edge between BSi and BSj is implemented by:

$$\tau_{ij} \leftarrow (1-\rho)\tau_{ij} \quad (3)$$

10. Before adding the P, the evaporation action has to be performed. The evaporation helps to find the shortest path and provide that no other path will be assessed as the shortest. This evaporation of pheromones has an intensity $\rho$.
11. If the BSs are not chosen by artificial ants, the amount of P decreases exponentially. Every moment of time, t={1,2,3,4…n}. After n

iterations, ants find the solution and leave the P calculated by the following formula:

$$\tau_{ij}(t+n) = \rho.\tau_{ij}(t) + \Delta\tau_{ij} \quad (4)$$

Here, $\Delta\tau_{ij}$ is the amount of pheromone being deposited.

12. If ant k has passed some edge between the BSs, it will leave P which is inversely proportional to the total length of all the edges. Ant k has passed from the starting BS to the end by using :

$$\tau_{ij} \leftarrow \tau_{ij} + \sum_{K=1}^{m} \Delta\tau_{ij}^{K},\ \forall(i,j) \in L. \quad (5)$$

$\Delta\tau ij^{k}$ is the amount of P ant k deposits on the edges visited. It is calculated by the following expression:

$$\Delta\tau_{ij}^{K} = \begin{cases} 1/C^{K} \\ 0 \end{cases} \quad (6)$$

where $C^{K}$ is the total length of all the edges

13. Now, the path with the best P value (minimum distance) is selected.
14. In the end, we will use a crossover operator to improve the communication path between CHs and BS.
15. Return.

### 2.2 Modified-signature-based trust evaluation

In this section, the modification of well-known signature-based trust evaluation is done with the help of three different weight factors. These weights factors are number weight, time decay weight, and context weight.

Formal expressions of modified signature and message: The modified signature generated by certifier for trust evaluation is denoted as

$$M_S(b,l) = I_C(b), I_C(l), T_x(b,l) C_m(b,l) R_V(b) T_S(b,l) D_s(b,l) \quad (7)$$

Here, $I_C(b)$ and $I_C(l)$ are the mean identification of certifier (b)and trustee (l), respectively. $T_x(b,l)$ denotes the type of corresponding message, $C_m(b,l)$ and $R_V(b)$ represent the rating value which is in the interval [0,28]. Larger $C_m(b,l)$ means higher satisfaction degree and vice versa. $R_V(b)$ represents the location coordinate of certifier (b) and $T_S(b,l)$ denotes the timestamp when the modified signature is generated. $D_s(b,l)$ represents the digital signature. The message released by the trustee (l) is denoted as:

$$T_m(l) = I_C(l), \acute{T}_m(l), \acute{C}_m(l), M_S(l), T_S(b,l), D_s(b,l) \quad (8)$$

Here, $I_C(l)$ denotes the identification of trustee node b. $\acute{T}_m(l)$ and $\acute{C}_m(l)$ stand for the type and content of the message, respectively. $M_S(l)$ denotes the set of modified signatures for trustee node b. $T_S(b,l)$ and $D_s(b,l)$ represent the timestamp and digital signature, respectively.

(a) Number weight: To balance the robustness against collision and bandwidth consumption, $M_S(l) \leq s2$ is the most favourable modified signatures which come from diverse certifiers. Here, $s2$ is a system parameter which relies on current network status regarding the collision. The number weight ($\acute{N}_w(l)$) corresponding to $\acute{T}_m(l)$ is denoted as a piecewise function:

$$\acute{N}_w(l) = \begin{cases} 0 & \text{if } M_S(l) < s2 \\ 1 & \text{otherwise} \end{cases} \quad (9)$$

If $n(f) \leq s2$, the modified signatures are considered incredible; thus, $\acute{N}_w(l)$is set to be 0. Otherwise, the modified signatures are viewed as reliable and $\acute{N}_w(l)$ is set to be 1.

(b) Time decay weight: Recently, evaluated modified signature value is more significant than previously available signature value. Therefore, the old modified signatures are unreliable. It is because the behaviour of a trustee may change from honest to malicious.

(c) Context weight: We also take the context weight into account for $\acute{C}_m(b,l)$. Specifically, we consider two kinds of most important contextual properties, namely message type and location.

(i) Message type: As we mentioned earlier, the node may first accumulate a high trust value through releasing authentic but unimportant messages. Then, it cheats the other nodes by issuing a relevant but unreal message. Therefore, we consider the message type similarity weight $I_C(b,l)$ for $T_x(b,l)$ as follows:

$$I_C(b,l) = \begin{cases} 1 \text{ if } m_{es}(T_x(b,l)) = m_{es}(I_C(l)) \\ \in \quad \text{otherwise} \end{cases} \quad (10)$$

Here, $m_{es}$ is an important function of message type and $\in$ is a constant within the range of [0, 1]. If the importance of $T_x(b,l)$ is not less than $I_c(b,l)$, then $\acute{C}_m(b,l)$ is considered reliable and $I_c(b,l)$ is set to 1. Otherwise, $\acute{C}_m(b,l)$ is regarded as not entirely credible and is set as $\in$.

(ii) Location: As discussed in earlier techniques Ambigavathi, et al. (2018), the location is also an important contextual property. In the view of trustor, the modified signature from a nearby certifier is more reliable than that from a remote certifier, as the latter has a high probability to join through trustee as compared to former. Thus, the location similarity weight LSW′ (b,z) between trustor (z) and certifier (b) is denoted as follows:

$$LSW'(b,z) = \begin{cases} 0 & \text{if } ||R_v(b) - R_v(z)|| . \rho \\ b^{||R_v(b) - R_v(z)|| . \vartheta} & \text{otherwise} \end{cases} \quad (11)$$

Here, $\rho$ is a distance threshold and $\vartheta$ is a constant which controls the speed of distance decay. If the distance between certifier (b) and z trustor exceeds $\acute{C}_m l$, then it is viewed as unreliable and $LSW^{'(b,z)}$ is set

as 0. Otherwise, $LSW'(b,z)$ is denoted as an exponential decay function of distance.

Trust calculation method: As stated in previous sections, the certifier [e.g. (b)] generates a modified signature (e.g. $M_S(b,l)$) and sent it to trustee (l). When trustee (l) needs to release a message $T_m(l)$, it first chooses $\acute{C}_m(l)$ most advantageous modified signatures from its local storage based on the weighted rating value $(w_r(b,l))$. It can be evaluated as:

$$w_r(b,l) = c_m(e,f) * D_W(B,L) * I_C(b,l) \quad (12)$$

It should be noted that in WSNs, the messages are usually broadcasted in a one-to-many manner. Thus, $w_r(b,l)$ is independent of $L_{SW}(b,l)$ in the proposed technique. When trustor z receives $T_m(l)$ it can extract $m(l)$ modified signatures and then calculate the modified-signature-based trust value $\acute{C}_m(b,l)$ of $T_m(l)$ using the following equation:

$$s_t(b,z) = \begin{cases} \frac{\sum_{a=1}^{m} C_{m(b,l)} \times D_{W(b,l)} I_C}{2*m} & if\ m(l) = R_v \\ \vartheta & \text{otherwise} \end{cases} \quad (13)$$

If $m(l)$ equals to $R_v$, the modified signatures are viewed as reliable, and $s_t(b,z)$ is calculated as the weighted average value c1 of ratings which come from different certifiers. Otherwise, the modified signatures are considered unreliable and $s_t(b,z)$ is set to low as a default value $(0 < \vartheta)$. From (8), we can easily find that $s_t(b,z)$ falls in the range of [0, 1]. In fact, the newly added trustees may have no sufficient modified signatures and malicious trustees may also act as newcomers and refuse to provide unfavourable modified signatures. Therefore, their modified-signature-based trust values are equal to $\vartheta$.

### 2.3 Recommendation-based trust evaluation

In this section, we have introduced the formation of a trust network based on recommendation-based trust evaluations. The recommendation-based trust evaluation has the ability to identify all trustworthy recommenders and present the details of recommendation-based trust calculation method.

The trust recommendation on trustee (l) is generated by recommender (n) for trustor (z) is denoted as follows:

$$\acute{R}_t(m,l_z) = I_C(m), I_C(l), I_C(z), C_m(m,lz), D_s(m,lz) \quad (14)$$

Here, $I_C(m)$, $I_C(l)$and $I_C(z)$ stand for the identifications of recommender n and trustee z, respectively. $C_m(m,lz)$ demonstrates the rating value and $D_s(m,lz)$ depicts the digital signature.

Formation of trust network: Owing to the sparse and highly dynamic characteristic, there are no sufficient or long-term trust relationships among nodes in WSNs. Thus, it calculates the trust values of receivers according to the accuracy and timelines of responses. Inspired by the previous work of Vijayalakshmi, et al. (2018), we adopt and improve the standard experience-based trust evaluation scheme Kanthimathi, et al. (2018).

Let $T_x(r,s) \in [0, 1]$ be trusted value demonstrating the satisfaction degree of sender to the responses of receiver R. If sender's p does not receive any response from receiver $T_x(r,s)$ is set to be 0. Whenever sender receives a response from receiver R, it updates $T_x(r,s)$ based on the following rules:

(i) If sender s is satisfied with the new response of receiver, $T_x(r,s)$ increases as follows:

$$T_x(r,s) = T_x(r,s) + \emptyset^*(1 - T_x(r,s) \quad (15)$$

(ii) Otherwise, $T_x(r,s)$ decreases as below:

$$T_x(r,s) = T_x(r,s)\# - \emptyset^* T_x(r,s) \quad (16)$$

Here, $\emptyset$ and $\#$ are the increment and decrement factors, respectively. Their ranges are [0,1]. Moreover, we set $\emptyset < \#$ because trust is difficult to build up but easy to drop off. We can quickly find that the experience-based trust is accumulated and trust values of nodes can be updated recursively as in Bano, et al. (2018). Moreover, the difficulty of the above calculations is small and each node can evaluate the trust values of other nearby nodes efficiently through testing interactions. Therefore, the trust network can be generated and dynamically updated in a lightweight manner.

Trust calculation method: In recommendation-based trust evaluation, only the ratings from trustworthy recommenders are considered. For identifying trustworthy recommenders, we propose a novel technique which calculates highest-restricted faithful standards related to recommenders in the view of trustor. As we know, trust network in WSNs has the highly dynamic characteristic. The reliability of trust evaluation may get extremely less if straight point gets much extended. Therefore, the consideration related to trust decays within the proposed procedure. Specifically, suppose $j_0 j_1 \cdots j_k$ where $j_0 = Z$, $j_k = 1$ and recommender l′ has previous interactions with trust z) is one of the optimal trust paths from trust or to recommender 1. Now, the highest confined faithful point $H_C(z,1)$ of recommender from the perspective of trustor can be obtained as:

$$H_C[z] = \begin{cases} \frac{\sum_{v=0}^{k=1} \bar{T}_v(i(v),i(v+1))}{k^{\emptyset}} & if\ k \le T_h(z) \\ 0 & otherwise \end{cases} \quad (17)$$

Here, k is the hop from trust or z to recommender l. $\phi$ is a parameter which controls the speed of trust decay. If $H_C[z]$ reaches the trust threshold $T_h(z)$ of trust or z, recommender l is viewed as a trustworthy and vice versa. Similarly, we can obtain all the elements of trustworthy recommender $(T_h(l,z))$ and calculate the recommendation-based trust $(\bar{R}_t(l,z))$ value (l) of a trustee in the view of trust or z as:

$$\bar{R}_t(l,z) = \begin{cases} \frac{\sum_{1 \in s_r} R_v(1f,Z)}{\sum_{1 \in s_r} H_C(Z)} & \text{if } s_r(l,z) \neq \emptyset \\ v & \text{otherwise} \end{cases} \quad (18)$$

If $s_r(l,z)$ = is not empty, $\bar{R}_t(l,z)$ is calculated as the weighted average value of ratings from all trustworthy recommenders. Otherwise, $\bar{R}_t(l,z)$ is set as a default low-value v ($0 < v < 1$). From (16) to (19), we can find that the range of $\bar{R}_t(l,z)$ is also [0, 1].

### 2.4 Integrated trust evaluation

As we have mentioned earlier, the signature and recommendation-based trust evaluations have diverse advantages and weaknesses as follows:

(a) Comparing to the recommendation-based trust evaluation, the modified-signature-based technique can be implemented in a faster and a lightweight manner.

(b) The recommendation-based trust evaluation seems to be more credible as compared to the modified-signature-based technique. As in the former, only ratings of trustworthy recommenders are considered. However, the collection of opinions from trustworthy recommenders consume large amounts of time and bandwidth resources. Therefore, it is beneficial to integrate these two kinds of trust evaluations to achieve the more accurate evaluation results. In the proposed scheme, the final trust value $f_t(l,z)$ of trustee ($l$) in sight of trustor ($z$) is calculated as below:

$$f_t(l,z) = w_p \times s_t(l,z) + 1(1 - w_p) \times T_t(l,z) \quad (19)$$

Here, $w_p$ is a weight parameter that controls the weight of two kinds of trust evaluations in aggregation. Therefore, the range of $f_t(l,z)$ lies in [0, 1].

## 3 PERFORMANCE EVALUATIONS

TO efficiently evaluate the performance of the proposed technique, the experimental platform is designed on MATLAB 2017a software with the help of wireless communication toolbox. All experiments are carried on an Intel Core-i5-520M Processor (3M Cache, 2.40 GHz) and 8-GB RAM. The parameter settings of the existing protocols are set as they are recommended in their original papers.

### 3.1 Integrated trust evaluation

We have run all the existing techniques and the proposed one on the same environment (i.e., MATLAB 2013a) with same number of standard parameters such as number of sensor nodes, Initial energy, Transmission and Receiver energy, free-space of multi-path energy etc. These parameters are obtained from the well-known Low energy efficient adaptive clustering hierarchy (LEACH) protocol. The parameters setting of the existing protocols is set as they are recommended in their original papers.

### 3.2 Performance analysis

To evaluate the efficiency of the proposed technique, three well-known quality metrics are considered in this paper. These are accuracy ($A_c$), f1 score ($f_m$), Matthews's correlation coefficient ($M_C$), Bandwidth analysis, and Execution time.

### 3.3 Experimental results

This section contains the experimental results of the existing and proposed wormhole detection techniques. The different number of nodes (i.e., 50–500) is tested on WSNs. However, the existing and the proposed techniques are not limited to these set of values.

Table 1 reveals that the wormhole recognition analysis of the proposed method along with the comparison of available well-known wormhole detection techniques. From Table 1, it has been clearly shown that the accuracy of the proposed technique is always more than that of the existing techniques. The mean improvement in accuracy is found to be 2.7489.

**Table 1.** Accuracy ($A_c$) analysis

| Nodes | Khalil et al.[10] | Su[12] | Qazi et al.[13] | Proposed technique |
|---|---|---|---|---|
| 50 | 86.016 | 88.156 | 92.205 | 94.761 |
| 100 | 87.100 | 89.138 | 90.115 | 94.066 |
| 150 | 86.011 | 87.125 | 91.997 | 95.106 |
| 200 | 89.936 | 90.198 | 92.296 | 95.190 |
| 250 | 85.867 | 88.224 | 89.643 | 94.953 |
| 300 | 90.188 | 91.173 | 92.531 | 96.645 |
| 350 | 87.122 | 88.641 | 89.898 | 94.887 |
| 400 | 85.118 | 89. 189 | 91.407 | 96.842 |
| 450 | 86.420 | 92.638 | 93.643 | 96.120 |
| 500 | 88.943 | 90.692 | 93.440 | 95.198 |

Table 2 shows that the proposed technique has better wormhole recognition rate in terms of (FS1) as compared to the existing techniques. It is observed that the mean improvement in terms of (FS1) is 0.1762.

**Table 2.** F-measure ($f_{m1}$)analysis

| Nodes | Nodes Khalil et al.[10] | Su[12] | Qazi et al.[13] | Proposed technique |
|---|---|---|---|---|
| 50 | 0.742 | 0.758 | 0.725 | 0.826 |
| 100 | 0.855 | 0.749 | 0.716 | 0.875 |
| 150 | 0.720 | 0.749 | 0.724 | 0.831 |
| 200 | 0.723 | 0.779 | 0.721 | 0.805 |
| 250 | 0.833 | 0.739 | 0.717 | 0.814 |
| 300 | 0.751 | 0.754 | 0.723 | 0.824 |
| 350 | 0.766 | 0.760 | 0.722 | 0.833 |
| 400 | 0.798 | 0.772 | 0.718 | 0.827 |
| 450 | 0.754 | 0.748 | 0.715 | 0.820 |
| 500 | 0.746 | 0.741 | 0.713 | 0.818 |

Table 3 shows that the proposed scheme has efficient kappa statistic ($\mathbf{k_{ps}}$) as compared to the existing techniques. From the table, it is observed that the mean improvement in terms of ($\mathbf{k_{ps}}$) is 2.781.

**Table 3.** Kappa statistic ($\mathbf{k_{ps}}$) analysis

| Nodes | Khalil et al. [10] | Su[12] | Qazi et al.[13] | Proposed technique |
|---|---|---|---|---|
| 50 | 0.4014 | 0.4826 | 0.5791 | 0.6492 |
| 100 | 0.4053 | 0.4126 | 0.5582 | 0.6490 |
| 150 | 0.4158 | 0.4243 | 0.5680 | 0.6395 |
| 200 | 0.4115 | 0.4335 | 0.5883 | 0.6506 |
| 250 | 0.4103 | 0.4229 | 0.5782 | 0.7401 |
| 300 | 0.4281 | 0.4389 | 0.5981 | 0.7292 |
| 350 | 0.4240 | 0.4521 | 0.5690 | 0.6190 |
| 400 | 0.4513 | 0.4627 | 0.5824 | 0.6488 |
| 450 | 0.4311 | 0.4751 | 0.5744 | 0.6512 |
| 500 | 0.4612 | 0.4803 | 0.5867 | 0.6422 |

Table 4 shows the bandwidth analysis of the existing and the proposed techniques. It is observed form the table that the proposed technique significantly utilizes the bandwidth as compared to the earlier techniques.

**Table 4.** Bandwidth analysis

| Nodes | Khalil et al. [10] | Su[12] | Qazi et al.[13] | Proposed technique |
|---|---|---|---|---|
| 50 | 0.9015 | 0.8829 | 0.8790 | 0.8498 |
| 100 | 0.9004 | 0.8723 | 0.8588 | 0.8495 |
| 150 | 0.9108 | 0.8842 | 0.8687 | 0.8397 |
| 200 | 0.9113 | 0.9134 | 0.8886 | 0.8505 |
| 250 | 0.9110 | 0.8828 | 0.8785 | 0.8401 |
| 300 | 0.9280 | 0.9287 | 0.8989 | 0.8298 |
| 350 | 0.9244 | 0.8925 | 0.8691 | 0.8193 |
| 400 | 0.9412 | 0.9027 | 0.8829 | 0.8499 |
| 450 | 0.9310 | 0.9124 | 0.8784 | 0.8504 |
| 500 | 0.9511 | 0.9300 | 0.8850 | 0.8403 |

In Table 5, analysis of execution time is demonstrated. Execution time (ET) is measured as the time (in seconds) taken to execute a given attack detection technique. The 'tic' and 'toc' operators in MATLAB script are used to compute ET. It can be seen from this table that the proposed technique takes less execution time as compared to the existing attack detection techniques. The mean reduction in ET by using the proposed technique over available techniques is approximately 0.2971.

**Table 5.** Execution time analysis

| Nodes | Khalil et al. [10] | Su[12] | Qazi et al.[13] | Proposed technique |
|---|---|---|---|---|
| 50 | 4.3645 | 3.3345 | 2.1988 | 1.9314 |
| 100 | 3.3262 | 2.3309 | 2.8957 | 2.6459 |
| 150 | 5.4115 | 4.3241 | 3.3199 | 2.7670 |
| 200 | 4.4834 | 3.2432 | 2.4311 | 2.1679 |
| 250 | 3.5231 | 3.2382 | 2.6281 | 2.1823 |
| 300 | 4.4300 | 2.3080 | 2.8909 | 1.1992 |
| 350 | 5.4412 | 4.3180 | 2.5619 | 1.2503 |
| 400 | 5.4730 | 4.3855 | 2.7866 | 2.2009 |
| 450 | 3.5810 | 3.3220 | 2.1504 | 1.0602 |
| 500 | 4.2811 | 3.3890 | 2.9612 | 1.5548 |

## 4 CONCLUSION

WSNs are easily susceptible to the wormhole attacks. The wormhole attacks are destructive against routing protocols which may drop messages or upset the communication path. In this paper, a novel wormhole attack detection technique is proposed for WSNs. In the proposed technique, a sensor can monitor and track the wormhole attackers with the help of the signature and the recommendation-based trust evaluation rules. Extensive experiments have shown that the proposed technique has detected wormhole attacks more efficiently with good computational speed as compared to the existing wormhole attack detection protocols.

## 5 ACKNOWLEDGMENTS

WE thank the faculty of Computer Science and Engineering Department of Khalsa College and my friends for their insightful comments and constructive suggestions to improve the quality of this research work.

## 6 REFERENCES

Ambigavathi, M. & D. Sridharan, (2018). Energy-Aware Data Aggregation Techniques in Wireless Sensor Network. *In Advances in Power Systems and Energy Management*. Springer, Singapore, 165-173.

Chuang, M., H. Liu, H., Zhou, Z. Wu, X. Yang and X. Xiao, (2011). A fault-tolerant algorithm of wireless sensor network based on recoverable nodes. *Intelligent Automation & Soft Computing 17*(6). 737-747.

Fan, T., L. Li, and Z. Jia, (2012). Improved shuffled frog leaping algorithm and its application in node localization of wireless sensor network. *Intelligent Automation & Soft Computing*. *18*(7), 807-818.

Giannetsos, T. & T. Dimitriou, (2014). A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks. Journal Computer Systems Science. 80(3), 618–643.

Han, Z., J. Wu and J. Zhang, (2014). A general self-organized tree-based energy-balance routing protocol for wireless sensor network. *IEEE Trans. Nucl. Sciences*. 61(2), 732–740.

Jen, H., C. Chen, S. Chen, W. Huang, Y. Chang and Y. Chen (2010). Conserving bandwidth in a wireless sensor network for telemedicine application. *Intelligent Automation & Soft Computing*. *16*(4), 537-551.

Ji, S., T. Chen and S. Zhong (2015). Wormhole attack detection algorithms in wireless network coding systems. *IEEE Trans. Mob. Compute*rs. 14(3), 660–674.

Jung, L., M. Soe, S. Chauhdary, S. Rhee and M. Park, (2017). A data aggregation scheme for boundary detection and tracking of continuous objects in WSN. *Intelligent Automation & Soft Computing*. 23(1), 135-147.

Kanthimathi, M., R. Amutha, and K. Senthil Kumar, (2018). Energy efficiency analysis of differential cooperative algorithm in wireless sensor network. *Cluster Computing*. 1-9.

Khabbazian, M., H. Mercier and K. Bhargava (2009). Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks. *IEEE Trans. Wirel. Commun*. 8 (2), 736–745.

Khalil, I., S. Bagchi and B. Shroff, (2007). Liteworp: detection and isolation of the wormhole attack in static multihop wireless networks. *Comput. Netw.*, 51(13), 3750–3772.

Li, W. & H.Song, (2016). An attack-resistant trust management scheme for securing vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Systems*. 17(4), 960–969.

Li, W., Song H., Zing F, (2017). Policy-based secure and trustworthy sensing for Internet of things in smart cities. *IEEE Internet of Things Journal*. 12(5).

Long, C., J. Niu, C. Luo, L. Shu, L. Kong, Z. Zhao, and Y. Gu, (2018). Towards minimum-delay and energy-efficient flooding in low-duty-cycle wireless sensor networks. *Computer Networks* 134, 66-77.

Madria, S. & J. Yin, (2009). A secure routing protocol against wormhole attacks in sensor networks, *Ad Hoc Netw*ork. 7(6), 1051–1063.

Mohanty, P. & R. Kabat, (2013). Wireless sensor networks: from theory to application (CRC Press), *Transport protocols in wireless sensor networks*. 265–306.

Mohanty, P. & R. Kabat, (2016). Energy efficient structure-free data aggregation and delivery in WSN, *Egypt" Inf. Journal*. 17(3), 273–284.

Nirnaya, P., K. Sharma, V. Singh and N. Tamang, (2018). TEECS: A Time-Based Energy Efficient Clustering Scheme in Wireless Sensor Networks. *In Advances in Electronics, Communication and Computing*. Springer, Singapore, 263-272.

Nishat, B., M. Alam, and S. Ahmad, (2018). Energy Efficient Image Compression Techniques in WSN. *In Intelligent Communication, Control and Devices*. Springer, Singapore, 1079-1088.

Poovendran, R. and L. Lazos, (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wirel. Network*. 13, (1), 27–59.

Pouryazdan, M., B. Kantarci and T. Soyata, (2016). Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing. *IEEE Access*. 4, 529–541.

Pouryazdan, M., B. Kantarci and T. Soyata, (2017). Quantifying user reputation scores, data trust worthiness, and user incentives in mobile crowd-sensing. *IEEE Access*. 5, 1382–1397.

Qazi, S., R. Raad, Y. Mu, (2013). Securing DSR against wormhole attacks in multirate ad hoc networks, *J. Netw. Comput. Applications*. 36(2), 582–592.

Qian, L., N. Song and X. Li, (2007). Detection of wormhole attacks in multi-path routed wireless ad hoc networks: a statistical analysis approach. *J. Netw. Comput. Appl*ications. 30(1), 308–330.

Rohini, R., and R. Gnanamurthy, (2016). Performance analysis to improve quality of service using cluster based hidden node detection algorithm in wireless sensor networks. *Intelligent Automation & Soft Computing*. *22* (2): 203-209.

Sajjad, H., M. Park, A. Bashir, S. Shah and J. Lee (2013). A collaborative scheme for boundary detection and tracking of continuous objects in WSNs. *Intelligent Automation & Soft Computing. 19* (3) 439-456.

Sharma, D., V. Kumar and R. Kumar (2016). Prevention of wormhole attack using identity based signature scheme in MANE. *Computational Intelligence in Data Mining*. 2, 475–485.

Singh, R., J. Singh and R. Singh (2016). A hybrid technique for detection of wormhole attack in wireless sensor networks. *Mob. Inf. Systems*. 20(8).

Singh, S., A. Malik, R. Kumar, (2016). Energy efficient heterogeneous DEEC protocol for enhancing lifetime in WSNs, *Eng. Sci. Technol., Int. Journal. 10(4)*.

Su, Y., (2010). WARP: a wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks, *Comput. Secur*ity. 29(2), 208–224.

Tian, B., Q. Li, Y. Yang, (2012). A ranging based scheme for detecting the wormhole attack in wireless sensor networks, *J. China University*. Posts Telecommun. 19, 6–10.

Vijayalakshmi, K., & P. Anandan, (2018). A multi objective Tabu particle swarm optimization for effective cluster head selection in WSN. *Cluster Computing*, 1-8.

Xia, W., Y. Xijun, and W. Xiaodong, (2012). Design of wireless sensor networks for monitoring at construction sites. *Intelligent Automation & Soft Computing*. *18* (6), 635-646.

Yao, X., X. Zhang and H. Ning, (2017). Using trust model to ensure reliable data acquisition in VANETs. *Ad Hoc Netw*orks. 55, 107–118.

Yousefi, H., H. Yeganeh and N. Alinaghipour (2012). Structure-free real-time data aggregation in wireless sensor networks. 35(9), 1132–1140.

Yun, J., I. Kim and H. Lim, (2007). Wodem: wormhole attack defense mechanism in wireless sensor networks. *Ubiquitous Convergence Technology*. Berlin Heidelberg, 200–209.

Zhang, D., S. Zhou, and J. Chen, (2017). New Dv-distance method based on path for wireless sensor network. *Intelligent Automation & Soft Computing*. *23*(2) 219-225.

## 7 DISCLOSURE STATEMENT

NO potential conflict of interest was reported by the authors.

## 8 NOTES ON CONTRIBUTORS

**Supreet Kaur** is a research scholar at Punjab Technical University. Her area of research is Wireless Sensor Networks. She has done M-Tech (CSE) from Dav College of Engineering and Technology, Jalandhar (DAVIET) and B-Tech (CSE) from Amritsar College of Engineering and Technology, Amritsar (ACET).

**Dr. Vijay Kumar Joshi** is a Professor in Computer Science & Engineering Department at I.K. Gujral Punjab Technical University, Jalandhar, India. He has many research papers in the field of Computer Science. His area of research is Wireless Sensor Networks and Network Security.