Integrated signature and recommendation-based trust evaluation protocol for wireless sensor networks

Supreet Kaur[1], *Rajiv Mahajan*[2]

[1]*Department of Computer Science and Engineering, IKG Punjab Technical University, Jalandhar, Punjab, India*
[2]*Golden College, Gurdaspur, Punjab, India*
E-mail: Oberoisupreet9@gmail.com

Published in *The Journal of Engineering*; Received on 1st July 2017; Accepted on 24th September 2017

Abstract: A wireless sensor network (WSN) is a wireless network containing of spatially distributed autonomous nodes utilising sensors to evaluate the physical or environmental circumstances. In several critical applications, an external user can directly monitor the real-time information from sensor nodes. In this case, before providing access, authenticity of the user is required to be proved by a suitable technique. Thus, in critical WSNs based real-time applications, authenticity of the users are very significant. Till now, many techniques have been developed to design a secure protocol for WSNs, to prevent unauthorised access. However, these techniques are vulnerable to wormhole attacks, which happen due to lesser synchronisation among the sensor nodes. Therefore, to handle this problem, an integrated modified-signature and recommendation-based trust evaluation protocol for WSNs is proposed. The extensive experiments have shown that the proposed technique outperforms over the available approaches.

1 Introduction

Wireless sensor networks (WSNs) are vulnerable to an extensive range of attacks due to their dispersed nature, lack of tamper resistance and limited sensor resources [1]. Several presents and envisaged applications for WSNs engage information gathering in remote, inaccessible or hostile circumstances such as ocean floors, barren region, mountains and battleground [2]. A huge number of sensors might be placed within a particular area, and their movement is frequently observed and supervised by a reliable, trusted unit, usually called sink or base station (BS) [3]. Owing to security issues and limited resource energy, WSNs are vulnerable to the attacks. So there is a need to provide adequate security mechanisms [4].

A wormhole attack is predominantly dangerous against routing in WSNs, whereas an attacker obtains data packets at one position in the network, tunnels and then replace them at a different remote position in sensor field [5]. A wormhole attack can be effortlessly initiated by an attacker without compromising any sensor node. As known prior, various routing approaches do not have mechanisms to protect the WSNs against wormhole attacks [6]. The path demand can be tunnelled to target sensor field by attacker using wormholes. Therefore, nodes in target sensor field construct the path using attacker. Afterwards, an attacker can alter/corrupt/drop the data packets [7].

A novel wormhole attack detection approach is designed using statistical analysis. In this technique, a sensor node can monitor and track wormhole neighbours using the neighbourhood discovery algorithm. Then, a *k*-means clustering is utilised to recognise wormhole attack [8]. Statistical analyses are also used to monitor wormhole attack in multi-path environment [9]. However, Tian *et al.* [8] and Qian *et al.* [9] become unsuccessful when prior information for statistical analysis is not available. A lightweight countermeasure is designed for wormhole attack depends on overhearing neighbour communication. This method allows monitoring of the wormhole attacker which is followed by isolation of the malicious nodes [10]. A novel lightweight countermeasure for wormhole attack detection is designed using localised–decentralised algorithm. It assures that no wormhole attack has happened while using connectivity data, as implied by the underlying communication graph [11].

A secure *ad hoc* on-demand distance vector routing protocol is proposed, so-called wormhole-avoidance routing protocol. It considers link-disjoint multi-path during route discovery, and provides greater route selections to avoid malicious nodes but eventually it uses only one path to transmit data [12]. A round trip time (RTT)-based wormhole attack detection technique is implemented. RTT secures WSNs against a wormhole attack for multi-rate transmissions [13]. A centralised method is designed to monitor wormholes. The proposed method guarantees a good lower bound of successful detection rate [14]. A time-based countermeasure is proposed to avoid the limitations of existing time-based wormhole attack detection. In this technique, neither the sensor nodes demand synchronised clocks, nor they request to predict the sending time. Therefore, they are capable for fast switching between the receiver and source nodes [15]. Wormhole resistant hybrid technique (WRHT)-based wormhole attack detection technique is proposed. WRHT utilises Watchdog and Delphi schemes and ensures that the wormhole will not be left untreated in WSNs [16].

Existing researchers have neglected the relation between the ratio of malicious users and the ratio of anchors in the WSNs event to ensure trustworthiness of the crowd-sensed data [17]. The impact of the relation between the ratio of malicious users, the ratio of anchors is also ignored [18]. The ratio of anchors on the crowdsourcer utility in the presence of anchor nodes in a WSN are also ignored [19]. 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 WSN [20].

Contribution: The review on existing security protocols of WSNs has shown that the detection of wormhole attack is still a challenging issue in WSNs. Most of the above-discussed protocols either demand specialised hardware or make strong assumptions to detect wormhole attacks, which limit the usability of these techniques. No protocol has good efficiency for detecting the randomisation behaviour of attackers. The utilisation of signature-based trust evaluation can improve the accuracy of wormhole attack detection. Therefore, we have proposed an integrated modified-signature and recommendation-based trust evaluation protocol (IMSRTEP). The proposed protocol has the following benefits over the existing signature-based protocols:

(i) Comparing to existing protocol, IMSRTEP can be implemented in a more fast and lightweight manner, while it is intuitively more vulnerable to collisions as certifiers are strange to the trustor in most cases.

(ii) IMSRTEP seems to be more significant than existing TEP, as in former only the ratings of trustworthy recommenders are considered. However, collecting the opinions from reliable recommenders, consumes large amount of time and bandwidth resources, especially when it is set to a relatively high value.

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

2 Proposed technique

This section describes the proposed technique. Initially, modified-signature-based trust evaluation is described. Then, recommendation-based trust evaluation is discussed. Fig. 1 shows step-by-step methodology of the proposed technique. Each step of the proposed technique plays a significant role to successfully detect the wormhole attacker node in WSNs.

2.1 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 factor weights are: number weight, time decay weight and context weight.

2.1.1 Formal expressions of modified signature and message: The modified signature generated by certifier for trust evaluation is denoted as in the below equation:

$$W_{\mathrm{C}}(e,f) = \mathrm{DI}_N(e), \mathrm{DI}_N(f), Y_{\mathrm{T}}(e,f)V_{\mathrm{R}}(e,f)C_{\mathrm{L}}(e)\mathrm{TI}_{\mathrm{S}}(e,f)S_{\mathrm{D}}(e,f) \quad (1)$$

where $\mathrm{DI}_N(e)$ and $\mathrm{DI}_N(f)$ are the mean identification of certifier (e) and trustee (f), respectively. $Y_{\mathrm{T}}(e, f)$ denote the type of corresponding message $V_{\mathrm{R}}(e, f)$ and $C_{\mathrm{L}}(e)$ represents the rating value which is in the interval $[0, 2^8]$. Larger $V_{\mathrm{R}}(e, f)$ means higher satisfaction degree and vice versa. $C_{\mathrm{L}}(e)$ represents the location coordinate of certifier (e) and $\mathrm{TI}_{\mathrm{S}}(e, f)$ denote the timestamp when the modified signature is generated. $S_{\mathrm{D}}(e, f)$ represents the digital signature. The message released by the trustee (f) is denoted as in the below equation:

$$S_{\mathrm{M}}(f) = \mathrm{DI}_N(f),\ Y_{\mathrm{M}}(f),\ C_{\mathrm{M}}(f),\ W_{\mathrm{C}}(f),\ \mathrm{TI}_{\mathrm{S}}(e, f),\ S_{\mathrm{D}}(e, f) \quad (2)$$

where $\mathrm{DI}_N(f)$ denotes the identification of trustee node b. $Y_{\mathrm{M}}(f)$ and $C_{\mathrm{M}}(f)$ stand for the type and content of the message, respectively. Also, $W_{\mathrm{C}}(f)$ denotes the set of modified signatures for trustee node b. $\mathrm{TI}_{\mathrm{S}}(f)$ and $S_{\mathrm{D}}(f)$ represent the timestamp and digital signature, respectively.

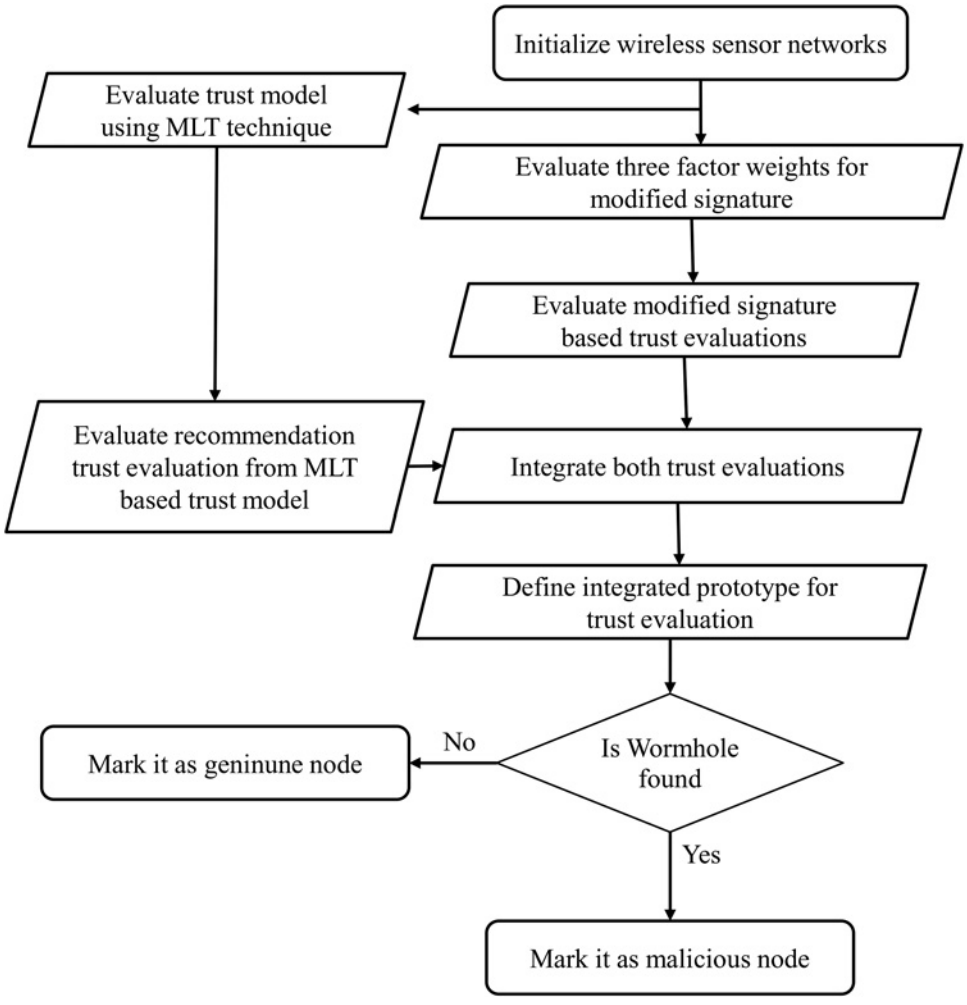

Fig. 1 *Diagrammatic flow of the proposed attack detection technique*

2.1.2 Three-factor weights for modified signature: Owing to the unique feature of the proposed protocol, trustee may merely provide profitable modified signatures to potential trustor or even collide with others to improve its trust value and slander its competitors (i.e. collision). Besides, the trustee may first accumulate high confidence value through releasing authentic but unimportant messages and cheat others by issuing necessary constraints. To ease these two kinds of messages, we comprehensively consider three-factor weights, which are number weight, time decay weight and context weight.

(a) Number weight: To balance the robustness against collision and bandwidth consumption, $W_C(f)$, merely consists of $M_S(f)$, ($M_S(f) \leq s1$) most favourable modified signatures which come from diverse certifiers. Here, $s1$ is a system parameter which relies on current network status regarding the collision. The number weight $N_W(f)$ corresponding to $M_S(f)$ is denoted as a piecewise function [12] below:

$$N_W(f) = \begin{cases} 0 & \text{if } M_S(f) < s2 \\ 1 & \text{otherwise.} \end{cases} \tag{3}$$

If $n(f) \leq s2$, modified signatures are considered incredible; thus, $N_W(f)$ is set to be 0. Otherwise, the modified signatures are viewed as reliable, so $N_W(f)$ is set to be 1.

(b) Time decay weight: Recently, evaluated modified signature value is more significant than previously available signature value. Therefore, old modified signatures are unreliable. It is because the behaviour of trustee may change from honest to malicious. Therefore, time decay weight $D_T(e, f)$ for $W_C(e, f)$ is calculated as follows:

$$D_T = \begin{cases} 0 & \text{if } N_T - S_T(e, f) > \beta \\ e^{-N_T - S_T(e,f)/\alpha} & \text{otherwise} \end{cases} \tag{4}$$

where N_T is the current timestamp and β is a time window. α is a time unit which controls the speed of time decay. If the time difference between N_T and $S_T(e, f)$ exceeds β, then $W_C(e, f)$ is considered as unreliable. Therefore, $D_T(e, f)$ is set to be 0. Otherwise, $D_T(e, f)$ is represented as an exponential decay function of a time difference.

(c) Context weight: We also take the context weight into account for $W_C(e, f)$. 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 high trust value through releasing authentic but unimportant message. Then, cheat the other nodes by issuing a relevant but unreal message. Therefore, we consider the message type similarity weight $Y_W(e, f)$ for $N_T(e, f)$ as in the below equation:

$$Y_W(e, f) = \begin{cases} 1 & \text{if } ms(Y_T(e, f)) = ms(Y_M(f)) \\ \gamma & \text{otherwise} \end{cases} \tag{5}$$

where $ms(\$)$ is an important function of message type and γ is a constant within the range of [0, 1]. If the importance of $Y_T(e, f)$ is not less than $Y_M(f)$, $W_C(e, f)$ it is considered reliable and $Y_W(e, f)$ is set as 1. Otherwise, $W_C(e, f)$ is regarded as not entirely credible and is set as γ.

(ii) Location: As discussed earlier techniques [1, 7, 14], the location is also an important contextual property. In the view of trustor, a 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 with former. Thus, location similarity weight $LS_{W'}(e, Z)$ between trustor Z and certifier (e) is denoted as follows:

$$LS(e, Z) = \begin{cases} O & \text{if } ||C_L(e) - C_L(Z)|| > \sigma \\ e^{||C_L(e) - C_L(Z)||\mu} & \text{otherwise)} \end{cases} \tag{6}$$

where σ is a distance threshold and μ is a constant which controls the speed of distance decay. If the distance between certifier (e) and Z trustor, $W_C(f)$ exceeds, is viewed as unreliable; thus $LS_{W'}(e, Z)$ is set as 0. Otherwise, $LS_{W'}(e, Z)$ is denoted as an exponential decay function of distance.

2.1.3 Trust calculation method: As stated in previous sections, the certifier [e.g. (e)] generates a modified signature (*e.g.* $W_C(e, f)$) and sent it to trustee (f). When trustee (f) needs to release a message, $S_M(f)$, it first chooses $M_S(f)$ most advantageous modified signatures from its local storage based on the weighted rating value ($W_R(e, f)$), which can be evaluated using the below equation:

$$W_R(e, f) = V_R(e, f)^* D_T(e, f)^* Y_W(e, f) \tag{7}$$

It should be noted that in WSNs, the messages are usually broadcasted in a one-to-many manner. Thus, $W_R(e, f)$ is independent of $LS_{W'}(e, Z)$ in the proposed technique.

When trustor Z receives $S_M(f)$, it can extract $n(f)$ modified signatures and then calculate the modified-signature-based trust value $W_C(f, Z)$ of $S_M(f)$ using the following equation:

$$S_T(f, Z) = \begin{cases} \dfrac{\sum_{a=1}^{n} V_R(e, f) \times D_T(e, f) \times Y_W(e, f) \times LS(e, Z)}{2 \times n} & \text{if } n(f) = c1 \\ \mu & \text{otherwise} \end{cases} \tag{8}$$

If $n(f)$ equals $c1$, the modified signatures are viewed as reliable, and $S_T(f, Z)$ is calculated as weighted average value $c1$ of ratings which come from different certifiers. Otherwise, the modified signatures are considered unreliable, and $S_T(f, Z)$ is set as a low default value ($0 < u1$). From (8), we can easily find that $S_T(f, Z)$ falls in the range of [0, 1]. In fact, 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 α.

2.2 Recommendation-based trust evaluation

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

2.3 Formal representation of trust-based recommendation

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

$$R_T(n, fZ) = DI_N(n),\ DI_N(f),\ DI_N(Z),\ V_R(n, fZ),\ S_D(n, fZ)$$

where $DI_N(n)$, $DI_N(f)$ and $DI_N(Z)$ stand for the identifications of recommender n and trustee Z, respectively. $V_R(n, fZ)$, demonstrates the rating value and $S_D(n, fZ)$ depicts the digital signature.

2.3.1 Formation of trust network: Owing to the sparse and highly dynamic characteristic, there are no sufficient or long-term trust

doi: 10.1049/joe.2017.0270

relationships among nodes in WSNs. To tackle this problem, we introduce 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 values of receivers according to the accuracy and time lines of responses. Inspired from the previous work [14, 15, 17], we adopt and improve the standard experience-based trust evaluation scheme [21].

Let $V_T(p, q) \in 0.1$ be trust value demonstrating the satisfaction degree of sender to responses of receiver r. If senders p do not receive any response from receiver q, $V_T(p, q)$ is set to be 0. Whenever sender receives a response from receiver r, it updates $V_T(p, q)$ based on the following rules:

(i) If sender s is satisfied with the new response of receiver $V_T(p, q)$ increases as in the below equation:

$$V_T(p, q) \leftarrow V_T(p, q) + \Phi^*(1 - V_T(p, q)) \tag{9}$$

(ii) Otherwise, $V_T(p, q)$ decreases as in the below equation:

$$V_T(p, q) \leftarrow V_T(p, q)\# - \Phi^* V_T(p, q) \tag{10}$$

where ϕ and # are the increment and decrement factors, respectively. Their ranges are [0, 1]. Moreover, we set $\phi < \#$ 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 [9, 10]. 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.

2.3.2 Trust calculation method: In recommendation-based trust evaluation, only the ratings from trustworthy recommenders are considered. For identifying trustworthy recommenders, we propose a novel IMSRTEP 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, and reliability of trust evaluation may get extremely less, if straight point gets much extended. Therefore, consideration related to trust decays within IMSRTEP procedure. Specifically, suppose $i_0 \to i_1 \to \cdots \to i_g$ (where $i_0 = Z$, $i_g = 1$ and recommender l' has previous interactions with trustee Z) is one of the optimal trust paths from trustor to recommender 1; now, highest confined faithful point $L_M(Z, 1)$ of recommender from the perspective of trustor can be obtained from [17] in the below equation:

$$L_M[Z] = \begin{cases} \dfrac{\sum_{v=0}^{g-1} \mathrm{TV}(i(v), i(v+1))}{g^{\theta}} & \text{if } g \le \mathrm{VG} \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

where g is the hop from trustor Z to recommender l' and *theta* is a parameter which controls speed of trust decay. If $L_M[Z]$ reaches the trust threshold $H_T(Z)$ of trustor Z, recommender l is viewed as trustworthy and vice versa. Similarly, we can obtain all the elements of trustworthy recommender set $S_R(f, Z)$ and calculate the recommendation-based trust $R_T(f, Z)$ value (f) of a trustee in the view of trustor Z as in the below equation:

$$R_T(f, Z) = \begin{cases} \dfrac{\sum_{1 \in S_R} R_V(1f, Z)}{\sum_{1 \in S_R} L_M(Z)} & \text{if } S_R(f, Z) \neq \Phi \\ V & \text{otherwise} \end{cases} \tag{12}$$

If $S_R(f, Z) \neq$ is not empty, $R_T(f, Z)$ is calculated as the weighted average value of ratings from all trustworthy recommenders. Otherwise, $R_T(f, Z)$ is set as a default low-value V ($0 < V < 1$). From (10) to (13), we can find that the range of $R_T(f, Z)$ is also [0, –1].

2.4 Integrated trust evaluation

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

(a) Comparing to recommendation-based trust evaluation, modified-signature-based one can be conducted in a more fast and lightweight manner while it is intuitively more vulnerable to the collision as the certifiers are strange to the trustor in most cases.
(b) Recommendation-based trust evaluation seems to be more credible than modified-signature-based one, as in the former only, ratings of trustworthy recommenders are considered. However, collecting the opinions from trustworthy recommenders consumes large amounts of time and bandwidth resources, especially when set to a relatively high value.

Therefore, it is beneficial to integrate these two kinds of trust evaluations to achieve the more accurate evaluation result. In the proposed scheme, the final trust value $F_T(f, Z)$ of trustee (f) in sight of trustor (Z) is calculated as in the below equation:

$$F_T(f, Z) = r_w \times S_T(f, Z) + 1(1 - r_w) \times T_T(f, Z) \tag{13}$$

where r_w is a weight parameter within range of which controls the weight of two kinds of trust evaluations in aggregation trust evaluation. Therefore, range of $F_T(f, Z)$ is also [0, 1]. Specifically, when r equals 1, ~0, the aggregation trust evaluation reduces to mere modified-signature-based one or mere recommendation-based one, respectively. In other cases, the aggregation trust evaluation falls in between modified-signature-based one and recommendation-based one.

3 Performance evaluation

To efficiently evaluate the performance of the proposed technique, experimental platform is designed in the MATLAB tool 2013*a*. The HP notebook computer is used with 8 GB random access memory and Intel core *i*5 processor.

3.1 Experimental set-up

The proposed and existing techniques are implemented by changing the nodes from 50 to 500. Initially, by running the simulation in normal environment we have taken the behaviour of nodes by considering certain factors along with whether or not they have done wormhole attack. This data is used to evaluate the accuracy of the proposed technique over the available wormhole attack detection techniques. The proposed technique is tested on well known general self-organised tree-based energy-balance RP (GSTEB) [23]. It constructs a routing tree by means of a method in which, for every round, BS chooses a root node and broadcasts this choice to each node. Then, every node chooses its parent node by taking into consideration just itself and its neighbours' information. This makes GSTEB a dynamic protocol. Goal of GSTEB is to

increase network lifetime of different applications. There are two definitions for network lifetime and two extreme cases of data fusion are considered in this paper under consideration which are described as follows:

A Network lifetime can be defined in two ways:
(a) The time from the beginning of the operation until first node dies.
(b) The time from the beginning of the operation until last node is dead.

B Also, two cases in data fusion are considered:

(a) *Case (1):* The data among sensor nodes can be completely fused. Every node transmits the same amount of data regardless of the amount it receives.
(b) *Case (2):* The data cannot be fused. Each relay node sends data which is an addition of its individually sensed data and data received from its child nodes.

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_Y), $F1$ score (F_{S_1}), and Matthews correlation coefficient (C_M). The mathematical formulas of these parameters are given below along with their detail.

3.2.1 Accuracy (A_Y): Accuracy (A_Y) refers to the similarity between calculated value to an actual value. In our case, binary cases are available in source data, which states that given node is attacker or not. Thus, a wormhole detection technique is said to be efficient if its maximum outputs are similar to the known results. A_Y always lies within [0, 100], close to 100 is required. It can be computed with the help of the following formula:

$$A_Y = \frac{(P_T + N_T)}{(P_T + N_T + P_F + N_F)} \tag{14}$$

In this P_T signifies correct analysis related to wormhole attack which has been identified adequately. P_F signifies the number of non-wormhole hops which have been identified successfully. While N_T represents all non-wormhole hops which have been estimated wrongly as wormhole. N_F shows the number of wormhole hops that have been identified to be authentic hops.

3.2.2 F-measure (F_{S_1}): F-measure so-called F1 score (F_{S_1}) shows the biased mean related to accuracy. It lies with the interval [0, 1]. Higher the value of (F_{S_1}) represents significant results of the given technique. Therefore, it should be maximised and can be calculated as

$$F_{S_1} = \frac{(2 \times P_T)}{(2 \times P_T + P_F + N_F)} \tag{15}$$

3.2.3 Kappa statistic (K_S): It evaluates precision related to any particular network along with precision related to arbitrary network. In this arbitrary precision has been considered as imaginary accepted possibility in suitable group based on previous restrictions. It can be determined using the following formula:

$$K_S = \frac{(A_Y - R_A)}{(1 - R_A)} \tag{16}$$

where random accuracy (R_A) can be written as below:

$$R_A = \frac{(N_T + P_F)^*(N_T + N_F) + (N_F + P_T)^*(P_F + P_T)}{(P_T + N_T + P_F + N_F)^2} \tag{17}$$

3.3 Experimental results

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

Authors' contributions:

(i) In this paper, first of all we have reviewed several existing wormhole attack detection techniques.
(ii) Then, we have evaluated and analysed their respective shortcomings.
(iii) Then, we have proposed a novel protocol which has integrated the features of SRTEPs. Therefore, it has ability to detect wormhole attack in more efficient way and with good speed.
(iv) The integration will be achieved by introducing a new prototype which will evaluate the confidence values based on rules of these two trust evaluation techniques.
(v) The proposed technique is designed and tested on several scenarios to validate the effectiveness of the proposed technique.

Table 1 and Fig. 2 reveal that the wormhole recognition analysis of the proposed method when compared with available well known wormhole detection techniques. From Table 1 and Fig. 2, it has been clearly shown that the accuracy of the proposed technique is always more than that of existing techniques. The mean improvement in accuracy is found to be 2.7489.

Table 2 and Fig. 3 show that the proposed technique has better wormhole recognition rate in terms of (F_{S_1}) when compared with

Table 1 Accuracy (A_Y) analysis

Nodes	Khalil *et al.* [10]	Su [12]	Qazi *et al.* [13]	Ji *et al.* [14]	Singh *et al.* [16]	Sharma *et al.* [21]	Li and Song [22]	Yao *et al.* [17]	IMSRTEP
50	88.0288	90.279	88.3288	88.0288	88.4488	83.0183	81.0981	76.6277	95.1995
100	89.1127	88.261	87.1277	87.1102	87.5414	82.2029	80.176	75.5341	94.0189
150	87.0129	91.137	88.2231	87.2087	89.3211	82.4122	80.238	75.7654	94.1078
200	90.1059	89.321	89.4198	90.3212	90.5153	81.2134	81.105	77.7561	95.2032
250	86.2101	92.347	87.7664	89.4210	88.5562	80.7324	79.217	76.4352	96.2187
300	87.3121	91.296	87.6546	87.1302	89.8773	81.3041	81.165	77.5471	95.1879
350	88.2451	88.764	89.2132	90.3129	87.5323	83.6711	80.223	76.6522	95.2121
400	91.1308	89.312	87.5313	89.4231	88.7672	80.1078	81.103	76.5564	96.2076
450	89.4330	87.761	88.7673	87.2421	87.2325	83.8217	80.089	77.5654	94.2435
500	90.2177	91.815	89.5643	88.1011	90.5762	82.7823	81.132	75.7564	95.3211

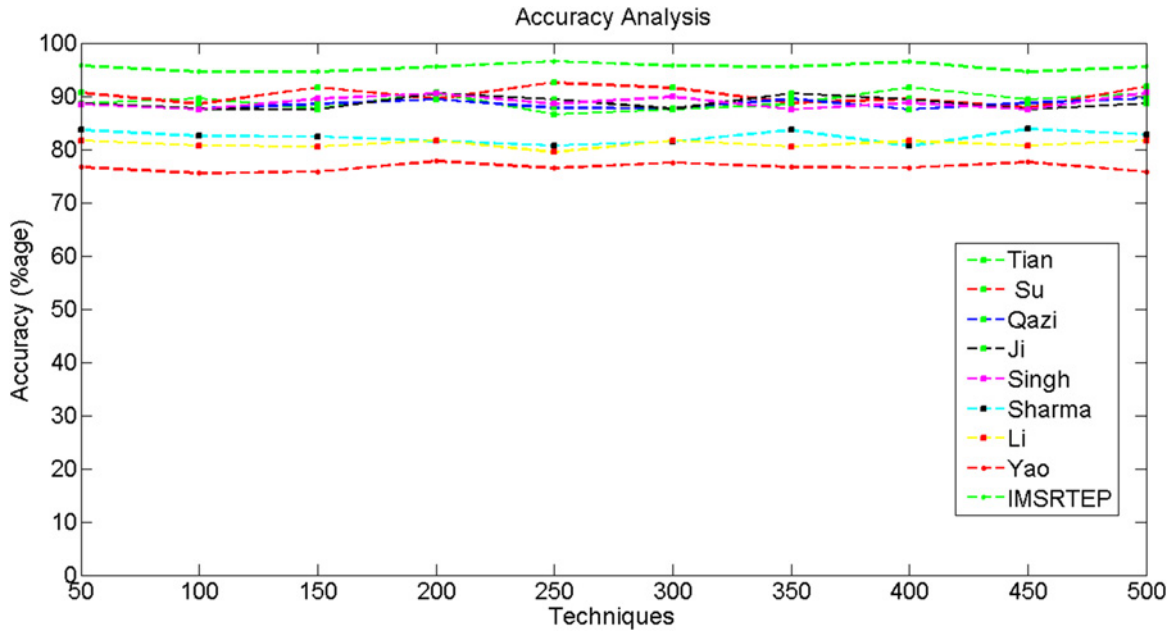

Fig. 2 *Accuracy (A_Y) analysis*

Table 2 F-measure (F_{S_1}) analysis

Nodes	Khalil *et al.* [10]	Su [12]	Qazi *et al.* [13]	Ji *et al.* [14]	Singh *et al.* [16]	Sharma *et al.* [21]	Li and Song [22]	Yao *et al.* [17]	IMSRTEP
50	0.865	0.881	0.848	0.865	0.85	0.753	0.74	0.679	0.949
100	0.978	0.872	0.839	0.857	0.84	0.741	0.76	0.667	0.998
150	0.843	0.872	0.847	0.859	0.83	0.750	0.73	0.642	0.954
200	0.846	0.902	0.844	0.862	0.86	0.749	0.70	0.681	0.928
250	0.956	0.862	0.840	0.860	0.82	0.753	0.71	0.680	0.937
300	0.874	0.877	0.846	0.855	0.87	0.748	0.75	0.659	0.947
350	0.889	0.883	0.845	0.861	0.88	0.747	0.72	0.680	0.956
400	0.921	0.895	0.841	0.864	0.82	0.754	0.69	0.676	0.950
450	0.877	0.871	0.838	0.853	0.80	0.752	0.68	0.668	0.943
500	0.869	0.864	0.836	0.854	0.81	0.751	0.77	0.675	0.941

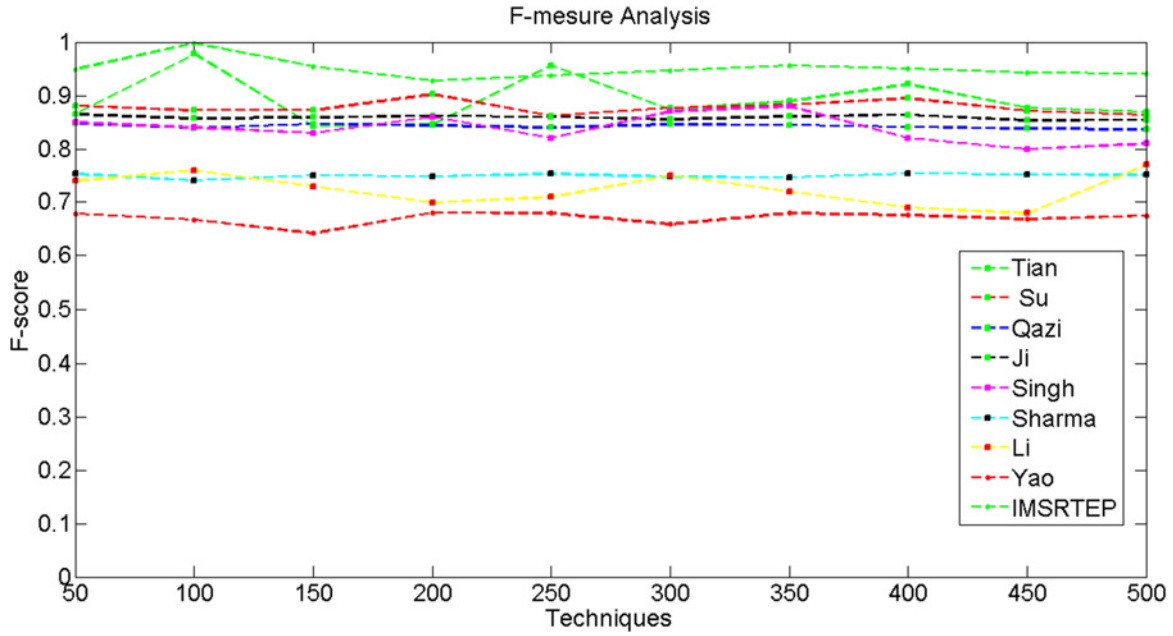

Fig. 3 *F-measure analysis*

doi: 10.1049/joe.2017.0270

Table 3 Kappa statistic (CC_M) analysis

Nodes	Khalil *et al.* [10]	Su [12]	Qazi *et al.* [13]	Ji *et al.* [14]	Singh *et al.* [16]	Sharma *et al.* [21]	Li and Song [22]	Yao *et al.* [17]	IMSRTEP
50	0.4049	0.4563	0.2924	0.4049	0.3033	0.59	0.1161	0.0911	0.7832
100	0.4038	0.4457	0.2922	0.4047	0.3032	0.61	0.1062	0.0892	0.7829
150	0.4042	0.4376	0.2921	0.4048	0.3030	0.56	0.1253	0.0909	0.7831
200	0.4047	0.4560	0.2920	0.4046	0.3034	0.62	0.1260	0.0913	0.7839
250	0.4044	0.4562	0.2919	0.4045	0.3031	0.67	0.1155	0.0915	0.7835
300	0.4041	0.4621	0.2923	0.4040	0.3135	0.51	0.1216	0.0890	0.7832
350	0.4050	0.4559	0.2925	0.4042	0.3036	0.53	0.1167	0.0904	0.7827
400	0.4046	0.4561	0.2936	0.4051	0.3029	0.68	0.1154	0.0919	0.7833
450	0.4044	0.4558	0.2918	0.4042	0.3028	0.69	0.1056	0.0917	0.7838
500	0.4045	0.4564	0.2927	0.4050	0.3037	0.57	0.1149	0.0910	0.7837

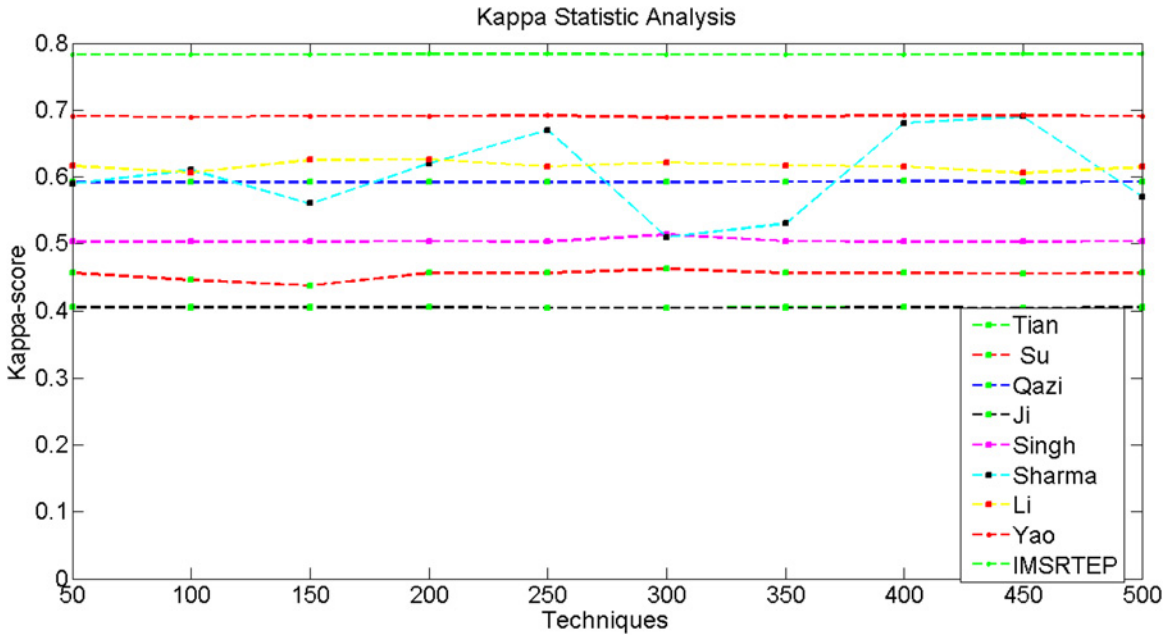

Fig. 4 *Kappa statistics analysis*

existing techniques. Table 2 and Fig. 3 have demonstrated that the mean improvement in terms of (F_{S_1}) is 0.1762.

Table 3 and Fig. 4 show that the proposed scheme has positive wormhole recognition (K_S) as compared with existing techniques. Table 3 and Fig. 4 have proved that the mean improvement in terms of (K_S) is 2.781.

4 Conclusion

WSNs are easily susceptible to wormhole attacks. The wormhole attack is destructive against routing scheme which may drop messages or upset communication path. In this paper, IMSRTEP is proposed to detect wormhole attack in an efficient way for WSNs. In IMSRTEP, a sensor can monitor and track the wormhole attackers with the help of signature and recommendation-based trust rules. Comparing to recommendation-based trust evaluation, IMSRTEP can be implemented in a more faster and lightweight manner. Extensive experiments have shown that the IMSRTEP outperforms over available 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

[1] Singh S., Malik A., Kumar R.: 'Energy efficient heterogeneous DEEC protocol for enhancing lifetime in WSNs', *Eng. Sci. Technol., Int. J.*, 2016, **20**, (1), pp. 245–253

[2] Mohanty P., Kabat M.R.: 'Energy efficient structure-free data aggregation and delivery in WSN', *Egypt. Inf. J.*, 2016, **17**, (3), pp. 273–284

[3] Mohanty P., Kabat M.R.: 'Transport protocols in wireless sensor networks', in El Emary I.M.M., Ramakrishnan S. (EDs.): 'Wireless sensor networks: from theory to applications' (CRC Press, 2013), pp. 265–306

[4] Yousefi H., Yeganeh M.H., Alinaghipour N., *ET AL.*: 'Structure-free real-time data aggregation in wireless sensor networks', *Comput. Commun.*, 2012, **35**, (9), pp. 1132–1140

[5] Madria S., Yin J.: 'SeRWA: a secure routing protocol against wormhole attacks in sensor networks', *Ad Hoc Netw..*, 2009, **7**, (6), pp. 1051–1063

[6] Poovendran R., Lazos L.: 'A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks', *Wirel. Netw.*, 2007, **13**, (1), pp. 27–59

[7] Yun J.-H., Kim I.-H., Lim J.-H., *ET AL.*: 'Wodem: wormhole attack defense mechanism in wireless sensor networks'. Ubiquitous Convergence Technology, Berlin Heidelberg, 2007, pp. 200–209

[8] Tian B., Li Q., Yang Y.-X., *ET AL.*: 'A ranging based scheme for detecting the wormhole attack in wireless sensor networks', *J. China Univ. Posts Telecommun.*, 2012, **19**, pp. 6–10, Supplement 1

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

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

[11] Giannetsos T., Dimitriou T.: 'LDAC: a localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks', *J. Comput. Syst. Sci.*, 2014, **80**, (3), pp. 618–643

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

[13] Qazi S., Raad R., Mu Y., *ET AL.*: 'Securing DSR against wormhole attacks in multirate ad hoc networks', *J. Netw. Comput. Appl.*, 2013, **36**, (2), pp. 582–592

[14] Ji S., Chen T., Zhong S.: 'Wormhole attack detection algorithms in wireless network coding systems', *IEEE Trans. Mob. Comput.*, 2015, **14**, (3), pp. 660–674

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

[16] Singh R., Singh J., Singh R.: 'WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks', *Mob. Inf. Syst.*, 2016, **2016**, (1), pp. 1–13

[17] Yao X., Zhang X., Ning H., *ET AL.*: 'Using trust model to ensure reliable data acquisition in VANETs', *Ad Hoc Netw.*., 2017, **55**, (1), pp. 107–118

[18] Pouryazdan M., Kantarci B., Soyata T., *ET AL.*: 'Anchor-assisted and vote-based trustworthiness assurance in smart city crowdsensing', *IEEE Access*, 2016, **4**, pp. 529–541

[19] Pouryazdan M., Kantarci B., Soyata T., *ET AL.*: 'Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing', *IEEE Access*, 2017, **5**, pp. 1382–1397

[20] Li W., Song H., Zeng F.: 'Policy-based secure and trustworthy sensing for Internet of things in smart cities', *IEEE Internet of Things J.*, 2017, **PP**, (99), pp. 1–1, DOI: 10.1109/JIOT.2017.2720635

[21] Sharma D., Kumar V., Kumar R.: 'Prevention of wormhole attack using identity based signature scheme in MANET'. Computational Intelligence in Data Mining, India, 2016, vol. **2**, pp. 475–485

[22] Li W., Song H.: 'ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks', *IEEE Trans. Intell. Transp. Syst.*, 2016, **17**, (4), pp. 960–969

[23] Han Z., Wu J., Zhang J., *ET AL.*: 'A general self-organized tree-based energy-balance routing protocol for wireless sensor network', *IEEE Trans. Nucl. Sci.*, 2014, **61**, (2), pp. 732–740