IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 1, 2019, accepted December 14, 2019, date of publication December 18, 2019,
date of current version December 30, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2960609

A Novel Trust Evaluation Process for Secure Localization Using a Decentralized Blockchain in Wireless Sensor Networks

TAI-HOON KIM[1], REKHA GOYAT[2], MRITUNJAY KUMAR RAI[2], GULSHAN KUMAR[3,5], WILLIAM J. BUCHANAN[4], RAHUL SAHA[3,5], AND REJI THOMAS[5,6]

[1]School of Economics and Management, Beijing Jiaotong University, Beijing 100044, China
[2]School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara 144411, India
[3]School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India
[4]Blockpass ID Lab, Edinburgh Napier University, Edinburgh EH10 5DT, U.K.
[5]Division of Research and Development, Lovely Professional University, Phagwara 144411, India
[6]School of Chemical Engineering and Physical Sciences, Lovely Professional University, Phagwara 144411, India

Corresponding author: Gulshan Kumar (gulshan3971@gmail.com)

ABSTRACT In this research paper, blockchain-based trust management model is proposed to enhance trust relationship among beacon nodes and to eradicate malicious nodes in Wireless Sensor Networks (WSNs). This composite trust evaluation involves behavioral-based trust as well as data-based trust. Various metrics such as closeness, honesty, intimacy and frequency of interaction are taken into account to compute behavioral-based trust of beacon nodes. Further, the composite (behavior and data) trust value of each beacon nodes is broadcast to Base Stations (BS) to generate a blockchain of trust values. Subsequently, the management model discards the beacon node with least trust value and that ensures reliability and consistency of localization in WSNs. The simulated results of the proposed algorithm are compared with the existing ones in terms of detection accuracy, False Positive Rate (FPR) and False Negative Rate (FNR) and Average Energy Consumption (AEC).

INDEX TERMS Beacon nodes, blockchain, localization, security, trust.

I. INTRODUCTION

Due to the advancement in technology and networking, the Internet of Things (IoT) becomes an emerging scenario which encourages various social and economic developments [1]. Wireless Sensor Networks (WSNs) play a key role with practical significance and research value in the rapid development of IoT. WSNs are ad hoc networks which are a collection of small devices embedded with sensing capabilities called sensor nodes. Sensor nodes should have the characteristics of large coverage area, monitoring with high precision, self-organization, random deployment, and fault-tolerance, etc., [2]. The autonomous sensor nodes are deployed surrounding area of interest to monitor happening physical activities. The gathered information is forwarded to the Base Station (BS) - or sink node - to perform computation through a wireless medium. WSNs have prospective applications in various fields such as military, surveillance, habitat monitoring, automation, disaster application, monitoring in healthcare, smart home and industrial applications [3]–[5]. Some applications need the precise location of the sensor nodes to make gathered data meaningful such as forest fire detection, target tracking, surveillance, and battlefield environments. The process of locating the sensor nodes is called localization [6]. Various localization algorithms have been developed by the researchers to achieve more precise localization in the last two decades [7], [8].

Due to remote or hostile operating environments and limited resources, to procure more precise localization is still a challenging issue. The localization process is affected by various attacks performed by malicious nodes makes it difficult to accomplish accurate location of nodes in WSNs. As already discussed above that localization play an important role in various applications in WSNs, but accurate localization in non-trusted environments is a challenging concern. Various secure localization algorithms have been developed to mitigate different malicious attacks. However, these algorithms have different shortcomings [9]. In this regard, the literature

The associate editor coordinating the review of this manuscript and approving it for publication was Luis Javier Garcia Villalba.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

of related researches is accomplished into two sections i.e. secure localization algorithm and emerging blockchain technology.

Collaborative Secure Localization based on Trust (CSLT) algorithm is shown in [10] for Underwater WSNs. The trust values of beacon nodes are evaluated for secure localization of unknown nodes. The Quality of Service (QoS) is predicted using collaborative filtering in service and mobile computing [11], [12]. Trust-Based Secure Localization (TBSL) algorithm is proposed for WSNs in which beacon nodes trust are evaluated by identifying the characteristics and behavior of nodes. The unknown nodes discover their locations using location information of credible beacon nodes [13]. Beta Reputation-based robust Secure Localization (BRSL) algorithm has been developed in which the trust evaluation is achieved based on beta reputation. Further, the locations of unknown nodes are estimated using a weighted Taylor-series least square method [14].

Another variation of secure algorithms based on trust for secure routing, malicious node detection, and intelligent transportation have been developed in WSNs [15]–[17]. Improved DV-Hop localization algorithm has been developed for WSNs in which faulty sensor nodes are detected to improve the localization accuracy [18]. Another Agent-based Secured Routing techniques is shown in [19] for WSNs based on trust values of sensor nodes. The information to remote nodes is broadcasted through trustworthy sensor nodes. A secure localization algorithm based on mutual authentication has been introduced in [20] for WSNs where malicious beacon nodes are detected in the network. Another secured localization algorithm based on Maximum Likelihood Estimation (MLE) has been shown in [21] to detect wormhole attacks within the network. The malicious nodes are identified using authentication based distance estimation and the location of sensor nodes are discovered using MLE. Another wormhole detection schemes are shown in [22], [23] based on Multi-Dimensional Scaling (MDS) with Round Trip Time (RTT) for WSNs.

The emerging blockchain technology gives a great impact on the Internet of Things (IoT) which enables the secure transaction, interaction, decentralization for improving the performance of the system [24]–[26]. A Blockchain-based Anonymous Reputation System (BARS) and certificate revocation schemes have been shown in [27], [28] to provide security in VANETs. Also, the blockchain technology based trusted routing, data storage and memory optimization schemes have been developed in [29]–[31] for WSNs. Another Blockchain-based trust model has been developed in VANETs for trust and privacy management of the vehicles. The direct and indirect reputation ensures the trustworthiness of the vehicles using the certificate and revocation transparency with blockchain [32], [33]. Emerging blockchain technology is also adopted in healthcare, cloud, and fog computing application for the privacy-preserving purpose [34], [35]. Therefore, incorporation of blockchain technology for trust management and secure localization is a new concept for WSNs. The main contributions of the present research paper are:

i) A blockchain-based trust management model is proposed to ensure the secure localization in WSNs.
ii) The trust value of each beacon nodes is aggregated based on behavioral-based trust and data-based trust.
iii) The composite trust values are broadcasted to BS to generate blockchain-based trust model.
iv) The location of unknown nodes is computed by using information of most trusty beacon nodes.

The rest of the research paper is structured as follows. Section 2 describes the proposed network model of the current research article. In Section 3, simulation of the proposed algorithm is presented and finally, the concluded remarks and future scope of the study are explained in Section 4.

II. PROPOSED NETWORK MODEL

In WSNs, localization is suffering from various problems such as location estimation issues, which affect the accuracy of localization, energy conservation problem which affects WSNs lifetime and malicious activity or attacks which may incur false location estimation. Therefore, to protect localization from malicious attacks with the least energy consumption, a blockchain-based trust management model is proposed in this paper.

A. NETWORK ENVIRONMENT

In network environment, sensor nodes are modeled by a undirected graph $G(V, E)$ where V represents the set of N nodes and E denotes the edge set of G. A set of N sensor nodes have b beacon nodes (BN) and n unknown nodes (UN) and m malicious beacon nodes (MN). The overall sensor nodes are represented using as following:

$$\begin{aligned} |N| &= |B| + |n| \\ \text{where } |B| &= |b| + |m| \end{aligned} \tag{1}$$

The sensor nodes which are forcefully and intentionally captured by attackers are called malicious nodes. Also, a BS is deployed at the center of the networks which controls the overall activity and mechanism of the network. All sensor nodes and BS are deployed in two-dimensional area A with a of $L \times L$, where L represents the length of each sides. The transmission range of each sensor node is circular and center of the circle represents the sensor node itself. BS is assumed most privileged in terms of resources, storage and communication and all the major task of localization computing is performed by BS. Each beacon node can communicate with BS and forwards location information and trust information to BS directly.

B. ADVERSARY MODEL

Various characteristics of the WSNs make it challenging to design an effective and efficient trust management model:

- An adversary can capture or compromise any beacon node and can forge the real identity or location of beacon nodes.
- An adversary has high performance hardware, more computational power and sensing capability than a normal sensor node.
- An adversary or malicious nodes can eavesdrop the location information of beacon nodes and forwards the false information to other sensor nodes.

Different types of malicious threats are:

- **Broadcasting false location information**. In this threat, the malicious node gains control over beacon nodes and then the victim node broadcast the false information about the location. Such type of information received by unknown nodes may cause more of a localization error during localization process. Hence, the estimated position of unknown nodes may be error-prone and inaccurate. An example of localization process of sensor nodes is shown in Figure 1 with false beacon information. The false position of beacon node B1 is represented by $B_1^{"}$ and the position of unknown node U1 is wrongly estimated at $U1^*$.

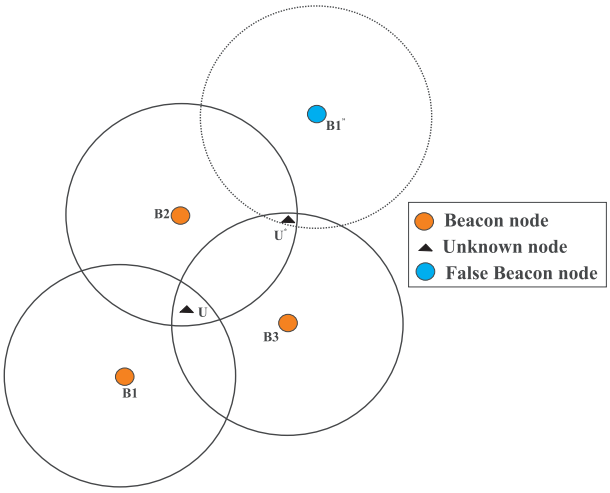

FIGURE 1. Sensor localization example in hostile environments.

- **Impersonation**. In this type of attack, an adversary produces its identity as a genuine node in the network and broadcasts false location to other sensor nodes. A malicious node spoofs the identity of legitimate beacon nodes in localization and proves itself as a part of legal nodes. In Figure 2, malicious node M1 spoofs the identity of beacon node B1 and broadcast the position of B1 across the network.
- **Tampering with the integrity of information**.
- **Reports false energy information to misguide the trust evaluation process**.
- **An attacker can receive all the information lies in the area of compromised nodes**. Consequently, the proposed trust model needs to deal with potential threats that result from the aforementioned attacks to improve the accuracy and security in the localization process.

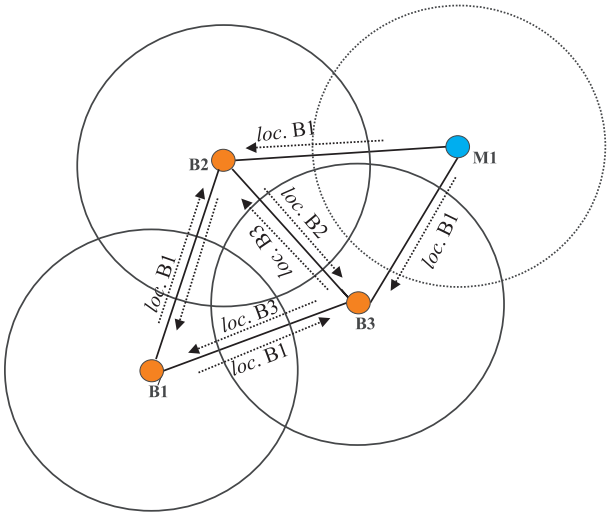

FIGURE 2. Example of Impersonation attack.

C. BLOCKCHAIN-BASED TRUST MANAGEMENT MODEL

The whole process of trust management is illustrated in Figure 3. The trust value of individual beacon nodes is evaluated in order to discard the malicious nodes. The format of Beacon packet is shown in Table 1

TABLE 1. Beacon packet format.

Id_i	Identification of i^{th} beacon node
X_i, Y_i	Location of beacon node
Timestamp	Timestamp when packet is generated
LON	List of Neighbors
Hop_{count}	Hop count between nodes

Therefore, interactions and collaborations among beacon nodes are employed to evaluate the trust value of each beacon node which is deduced by node location information, node behavioral trust and data trust. The trust evaluation process is shown in Figure 4.

1) TRUST EVALUATION PROCESS

The process of trust evaluation is divided into three parts: i) Behavioral-based trust ii) Data-based trust iii) Feedback based Trust and explained in detailed as following:

- **Behavioral-based trust evaluation**
  Behavioral-based trust is evaluated based on various metrics such as closeness, honesty, intimacy, frequency of interaction and feedback of nodes are discussed as follows:

1) Closeness:
Closeness ($D_i^{closeness}$) is a metric that is used for trust value evaluation. It is represented by how many total

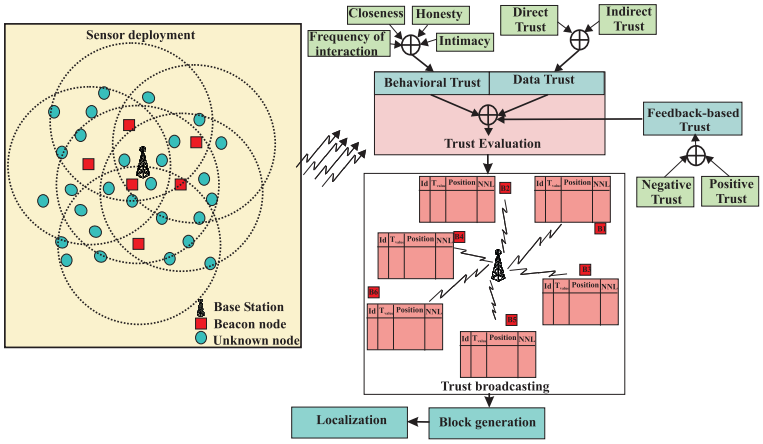

FIGURE 3. Blockchain-based trust management model.

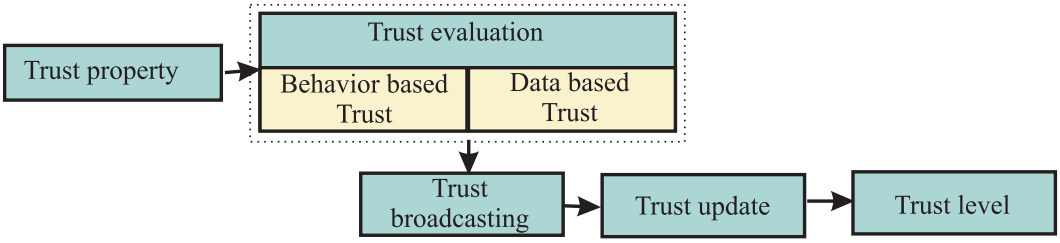

FIGURE 4. Trust evaluation process.

number of sensor nodes are covered by each beacon node in one-hop neighbored and is computed as following:

$$D_i^{closeness} = \frac{\sum_{j=1,i\neq j}^{N} D_{ij}^{one-hop}}{\sum_{j=1,i\neq j}^{N} D_{ij}^{max-hop}} \tag{2}$$

where $\sum_{j=1,i\neq j}^{N} D_{ij}^{one-hop}$ represents the total one-hop neighbor nodes covered by i^{th} beacon node and $\sum_{j=1,i\neq j}^{N} D_{ij}^{max-hop}$ is the all sensor nodes present in the network except by i^{th} beacon node.

2) Honesty:
Another important metric for behavioral-based trust evaluation is honesty ($D_i^{honesty}$). Honesty is defined by number of successful and unsuccessful interaction among sensor nodes and its value lies within [0, 1] i.e. $D_i^{honesty} \in [0, 1]$. ($D_i^{honesty} = 0$) and ($D_i^{honesty} = 0$) represents the trustworthy beacon node and malicious beacon node respectively. $D_i^{honesty}$ is computed as following:

$$D_i^{honesty} = \frac{I_{i,j}^{successful}}{I_{i,j}^{successful} + I_{i,j}^{unsuccessful}} \tag{3}$$

where $I_{i,j}^{successful}$ and $I_{i,j}^{unsuccessful}$ represents the total successful and unsuccessful interaction between beacon nodes.

3) Intimacy:
Another metric for trust evaluation is intimacy $D_i^{Intimacy}$ which represents the time of interaction between beacon nodes and higher time of interaction signifies higher intimacy. $D_i^{Intimacy}$ of i^{th} beacon node is computed as following:

$$D_i^{Intimacy} = \frac{t_{ij}}{t_{ij} + t_{ik}} \tag{4}$$

where t_{ij} and t_{ik} represents the total time of interaction with beacon node j and k respectively.

4) Frequency of Interaction (FI):
FI ($I_i^{Frequency}$) is also an important trust metric for trust evaluation which represents the total number of interaction between beacon nodes. Higher value of FI represents the closely relationship between nodes. $I_i^{Frequency}$ is computed as following:

$$I_i^{Frequency} = \frac{n_{ij}}{n_{ik}} \tag{5}$$

n_{ij} defines the number of interaction between beacon node i and j and n_{ik} is the total number of interaction with other k beacon nodes. Overall behavioral trust value of beacon nodes is evaluated as following:

$$Trust_{Behavioral}(i) = w_1 \times D_i^{closeness} + w_2 \times D_i^{honesty} + w_3 \times D_i^{Intimacy} + w_4 \times I_i^{Frequency} \tag{6}$$

$$w_1 + w_2 + w_3 + w_4 = 1 \tag{7}$$

- **Feedback-based trust evaluation**
The feedback based trust also ensures the integrity of each beacon nodes. To compute the feedback based trust,

the feedback trust is classified into two categories such as positive feedback and negative feedback. Let us consider a set B $(b_1, b_2, ..., b_M)$ of beacon nodes are deployed in the network. When the beacon node receives the location information from neighbor beacon nodes, it provides the feedback about the sender nodes. In the proposed trust model, the range of both feedbacks lies in the range of [0, 1]. The feedback value between (0.5, 1) is termed as positive feedback and the value in (0, 0.5) termed as negative feedback. Initially, 0.5 is the feedback value considered for all beacon nodes. $F^i_{positive}$ and $F^i_{negative}$ are the total number of positive and negative feedbacks for i^{th} beacon node. By considering these assumptions, the feedback values for i^{th} beacon node are defined as:

$$\text{Beacon node feedback:}\{F^i_{positive}, F^i_{negative}\}$$

Now, the feedback based trust (F^i_{Trust}) for each beacon node is evaluated in following sections.

Trustworthiness computation:

Initially, the location information packet of all beacon nodes $\{Beaconpacket : Id_i, (x_i, y_i), timestamp\}$ are broadcasted within neighboured nodes. The beacon node which broadcast its information act as a sender beacon denoted as $(Sender_{BN})$ and the nodes which provide the feedback about $Sender_{BN}$ are termed as $Responder_{BN}$. After receiving the packets, $Responder_{BN}$ provides its feedback about particular $(Sender_{BN})$ node. The creditability of beacon node is computed based on the Total Number of Feedback $(TNoF)$ provided for that particular beacon node.

1) **Positive feedback rate (PF^{rate}) computation:**

$$PF^{Rate}_{ij} = \frac{(P^i_F)}{(P^i_F + N^i_F)} \tag{8}$$

where P^i_F and N^i_F represents the number of positive and negative feedbacks respectively provided by the j^{th} beacon node for i^{th} beacon node. Higher the value of PF^{Rate}_{ij} represents the stronger the trust of j^{th} towards i^{th} node.

2) **Credibility $(credibility^i_{BN})$ computation based on PF^{rate}:**

PF^{rate} reflects the worthiness of the information provided by $Sender_{BN}$ in context of $Responder_{BN}$. Here, the value of PF^{rate} lies in between (0, 1) and various Type equation here.values of PF^{rate} reveals different values of trust for $Sender_{BN}$. The trust values of beacon nodes are computed by dividing PF^{rate} into following ranges:

a. PF^{rate} **in range of 0 to 0.2**
b. PF^{rate} **in range of 0.2 to 0.4**
c. PF^{rate} **in range of 0.4 to 0.6**
d. PF^{rate} **in range of 0.6 to 0.8**
e. PF^{rate} **in range of 0.8 to 1**

a) PF^{rate} **in range of 0 to 0.2**

PF^{rate} in this range reveals that $Responder_{BN}$ gave almost all feedback negative regards $Sender_{BN}$. In other words, we can say that $Responder_{BN}$ beacon node is not satisfied with the information provided by $Sender_{BN}$. Therefore, the value of $(credibility^i_{BN})$ is considered as zero.

b) PF^{rate} **in range of 0.2 to 0.4**

In this case, the $Responder_{BN}$ tended to provide the negative feedback to $Sender_{BN}$ based on past interactions. The creditability of $Sender_{BN}$ is computed as following:

$$credibility^i_{BN} = \frac{1}{|F^i_{negative}|} \times \sum_{i \in F^i_{negative}} negative\_credibility^i_{BN} \tag{9}$$

$$negative\_credibility^i_{BN} = \frac{1}{(N^i_F)} \times \sum_{j=i}^{N^i_F} feedback^i_j \times NTFF^i_j \tag{10}$$

$$NTFF^i_j = \frac{\{Time^i_j\}}{\sum_{l=1}^{N^i_F}(time_l - time_0)} \tag{11}$$

$credibility^i_{BN}$ is the trustworthiness of i^{th} beacon node computed by j^{th} node and $F^i_{negative}$ is the total number of beacon nodes which provide negative feedback to i^{th} beacon node in past. N^i_F is the number of negative feedback given by j^{th} node out of $F^i_{negative}$, $feedback^i_j$ represents the feedback regards given by j^{th} node out of $F^i_{negative}$ and $NTFF^i_j$ represents the negative time fading factor. $time_0$ is the time when node start to compute the credibility and $time_l$ is the time after computing the credibility.

c) PF^{rate} **in range of 0.4 to 0.6**

In this situation, $Responder_{BN}$ fluctuates in between good and bad behaviour of the $Sender_{BN}$ due to past interactions. In such type circumstances, both the positive and negative credibility of $Sender_{BN}$ is considered as following

$$credibility\_BN^i = \frac{1}{2}\left(\frac{1}{|F^i_{positive}|} \times \sum_{i \in F^i_{positive}} positive\_credibility^i_{BN} + \frac{1}{|F^i_{negative}|} \times \sum_{i \in F^i_{negative}} negative\_credibility^i_{BN}\right) \tag{12}$$

d) PF^{rate} **in range of 0.6 to 0.8**
In this case, the $Responder_{BN}$ tended to provide the positive feedback to $Sender_{BN}$ based on past interactions and the credibility is computed as following:

$$credibility^{i}_{BN} = \frac{1}{|F^{i}_{positive}|} \times \sum_{i \in F^{i}_{positive}} positive\_credibility^{i}_{BN} \quad (13)$$

$$positive\_credibility^{i}_{BN} = \frac{1}{(P^{i}_{F})} \times \sum_{j=i}^{P^{i}_{F}} feedback^{i}_{j} \times PTFF^{i}_{j} \quad (14)$$

$$PTFF^{i}_{j} = \frac{\{Time^{i}_{j}\}}{\sum_{l=1}^{P^{i}_{F}} (time_{l} - time_{0})} \quad (15)$$

$credibility^{i}_{BN}$ is the trustworthiness of i^{th} beacon node computed by j^{th} node and $F^{i}_{positive}$ is the total number of beacon nodes which provide positive feedback to i^{th} beacon node in past. P^{i}_{F} is the number of positive feedback given by j^{th} node in all $F^{i}_{positive}$, $feedback^{i}_{j}$ represents the feedback regards given by j^{th} node out of $F^{i}_{positive}$ and $PTFF^{i}_{j}$ is the positive time fading factor. $time_0$ and $time_l$ are the times when node start to compute the credibility and time after computing the credibility respectively.

e) PF^{rate} **in range of 0.8 to 1**
In such situation, all the feedbacks given by $Responder_{BN}$ towards $Sender_{BN}$ are positives. In other words, we can say that $Responder_{BN}$ was satisfied with the information provided by $Sender_{BN}$ in the past.

- **Data-based trust evaluation** Data-based trust is evaluated based on direct trust observation and indirect trust observation as shown in Figure 5 and explained as following:
- Direct trust observation:
The sender beacon nodes forward the location information to one-hop neighbors with the speed of light (c) with a timer start. The individual beacon nodes discover their one-hop neighbor nodes and enlist in Neighbor List (NL)4. When the information received from neighbor beacon nodes, the sender beacon node stops the timer and computes the estimated distance (D^{est}_{ij}) between beacon nodes using following equation:

$$D^{est}_{ij} = c \times RTT \quad (16)$$

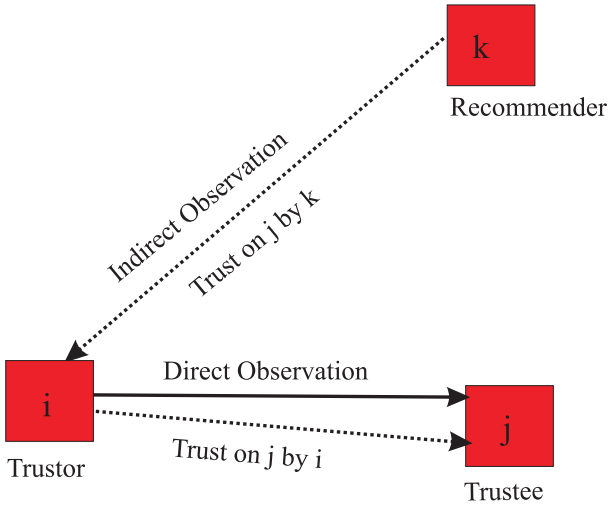

FIGURE 5. Data trust evaluation.

where RTT represents the Round Trip Time. RTT is computed as following:

$$RTT = T_{start} - T_{stop} \quad (17)$$

The true distance between beacon nodes is computed as following:

$$D^{act}_{ij} = \sqrt{(x_i + x_j)^2 - (y_i + y_j)^2} \quad (18)$$

where (x_i, y_i) and (x_j, y_j) represents the coordinates of beacon node i and beacon node j. Now the direct trust value (T^{i}_{Direct}) for each beacon node is computed as following:

$$T^{i}_{Direct} = \alpha \times T^{ij}_{t} + (1 - \alpha) \quad (19)$$

where T^{ij}_{t} represent the trust value of beacon node i by j at times t and initially the value of T^{ij}_{t} is set to 0.5. α represents the trust value which is computed as following:

$$\alpha = \frac{(\mid D^{act}_{ij} - D^{est}_{ij} \mid)}{(D^{act}_{ij} + D^{est}_{ij})} \quad (20)$$

- Indirect trust computation:
Indirect trust ($T^{i}_{indirect}$) value is computed when two beacon nodes do not have prior trust relationship and in this case the observer beacon nodes does not have the capability to judge the other beacon nodes. The sensor nodes that provide the trust value to other nodes are called recommender nodes.

$$T^{i}_{indirect} = \frac{\sum_{i=1}^{k} T^{ik}_{indirect}}{k} \quad (21)$$

For each beacon nodes, $Trust_{Data}$ is computed by combining both T^{ij}_{Direct} and $T^{i}_{Indirect}$ values with random weights w_{direct} and $w_{indirect}$ respectively and evaluated by using the following mentioned equation:

$$Trust_{Data}(i) = w_{direct} \times T^{i}_{Direct} + w_{indirect} \times T^{i}_{Indirect} \quad (22)$$

$$w_{direct} + w_{indirect} = 1 \tag{23}$$

Mathematically, the trust value of individual beacon node is computed by combining behavioral and data trust as following:

$$Trust_{total}(i) = Trust_{Behavioral}(i) + Trust_{Data}(i) \tag{24}$$

Algorithm 1 Trust value estimation

Deployment of M beacon nodes and n unknown nodes
Each beacon node B_i broadcast $(Id_i, x_i, y_i, Hop_{count} = 0)$ to B_j
B_i computes trust values of beacon node B_j
Total trust evaluation
if $Hop_{count} = 1$
$B_j^{closeness} = \frac{\sum_{(j=1,i\neq j)}^{N} D_{ij}^{(one-hop)}}{\sum_{(j=1,i\neq j)}^{N} D_{ij}^{(max-hop)}}$
else
$B_j^{closeness} = 0$
end if
$B_j^{honesty} = \frac{(I_{(i,j)}^{successful})}{(I_{(i,j)}^{successful} + I_{(i,j)}^{unsuccessful})}$
$B_j^{Intimacy} = \frac{t_{ij}}{(t_{ij}+t_{ik})}$
$B_j^{Frequency} = \frac{n_{ij}}{n_{ik}}$
for each beacon node B_j
$B_{Behavioural}^{Trust_j} = w_1 \times B_j^{closeness} + w_2 \times B_j^{honesty} + w_3 \times B_j^{Intimacy} + w_4 \times B_j^{Frequency}$
end for
for each beacon node B_j
$B_{Direct}^{Trust_j} = \alpha \times T_t^{ij} + (1 - \alpha)$
$B_{indirect}^{Trust_j} = \frac{\sum_{i=1}^{k} T_{indirect}^{ik}}{k}$
$B_{Data}^{Trust_j} = w_{direct} \times B_{Direct}^{Trust_j} + w_{indirect} \times B_{indirect}^{Trust_j}$
$B_{total}^{Trust_j} = B_{Behavioural}^{Trust_j} + B_{Data}^{Trust_j}$
end for

- **Life-Time Checking of past interactions**
  As we considered the network scenario for the localization process and mobility of nodes affects the performance of the process. Due to dynamic behaviour, the lifetime (L_{Time}) of the packets/interaction is also an important issue to concern. In other words, new arrival interactions are more reliable as compared to old/interactions in networks. Life-time of interactions is defined as the time interval between the Time of Event (ToE) and the Time of Expiration (ToEx) of the interaction. To mitigate the problem of the redundancy of old/interactions, Life-Time Checking (LTC) is introduced. The proposed scheme computes the difference between the ToE and Current Time of Interaction (CToI). A Threshold-ToE $\wp$ is further computed for interaction to provide more reliability to the proposed process. The value of $\wp$ is set to high in case of a low-density network or in sparse network scenario and it will be low under high dense networks. If the ToE is too old/expired, in such a case, the interaction must be discarded otherwise is should be utilized during trust computation and the process of Life-Time Checking is explained in Algorithm 2

Algorithm 2 Life-Time Checking

Input: (Interaction, $Time_{current}$, $Time_{event}$)
$Time_{difference} = Compute\_difference(Time_{current}, Time_{event})$
$Time_{threshold} = Extract\_threshold\_time(Time_{event})$
if $Time_{difference} > Time_{threshold}$
Discard interaction value
else
Go to next step

2) TRUST MANAGEMENT MODEL

After trust evaluation, all beacon nodes broadcast the NNL and trust value to BS. BS generates blockchain with trust values of individual beacon nodes for trust management and to detect malicious beacon nodes. Firstly, the information of the beacon node with higher trust value is selected as the first block of the blockchain. Beacon node with higher trust value has more probabilities to add blocks in the blockchain and the structure of each block in the blockchain in depicted in Figure 6. The information of beacon nodes with the least trust value is discarded and not included as a block in the blockchain. The proposed algorithm depends on the trust score of individual beacon nodes. The trustworthiness of beacon nodes is utilized during blockchain generation, and it cannot be spent or transferred as coins in Bitcoin. Higher trusty beacon nodes provide more superior and precise localization. When a malicious node is detected and discarded from blockchain, the trust value of each beacon node is updated and constructed in the blockchain.

3) LOCALIZATION OF SENSOR NODES

Finally, the location of unknown nodes is computed with the most trustworthy location information of beacon nodes. All the major task of localization process in performed at BS to reduce the energy consumption of beacon nodes. Minimum three beacon nodes are selected for each unknown nodes to perform trilateration process [36], and the most trusty location information of beacon nodes are utilized during localization for accurate localization.

III. SIMULATION RESULTS

The performance of the proposed algorithm is evaluated against B. B. Das et al., (2017) [18], T. Gaber et al. (2018) [17] and G. Han et al., (2016) [10] using MATLAB with Intel (R) Core(TM) i3-3217 CPU @1.80 GHz. The sensor nodes are considered stationary in nature for the simulation. The range of transmission for all sensor nodes is considered identical.

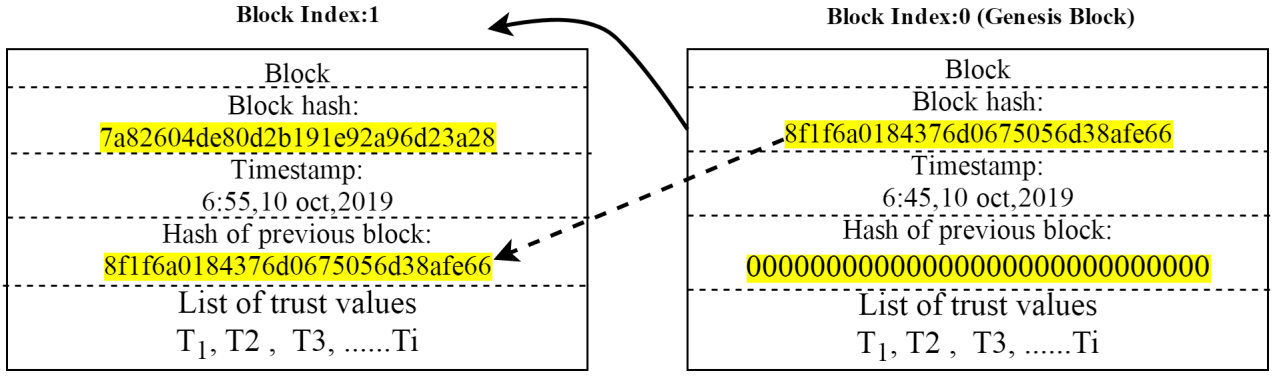

FIGURE 6. Structure of block in blockchain.

TABLE 2. Simulation parameters.

Parameters	Value of parameters
Sensing area	$100 \times 100\ m^2$
Total sensor nodes	100
Beacon nodes	5-30%
Hash algorithm	SHA-256
Malicious node	5-30% of beacon nodes
Initial energy	5J
Communication radius	20-40
Network topology	Random-way point distribution
Speed	0 to V_{max}

A. SIMULATION PARAMETERS AND PERFORMANCE METRICS

The value of parameters used in simulation is shown in Table 2. To evaluate the performance of the proposed algorithm various performance metrics are explained as follows:

1) **Localization Error (LE) and Average Localization error (ALE)**
The difference between estimated and actual position of unknown node is referred as localization error and computed as following:

$$LE = \sqrt{(x_j^{est} - x_j^{act})^2 + (y_j^{est} - y_j^{act})^2} \tag{25}$$

where (x_j^{exp}, y_j^{exp}) and (x_j^{exp}, y_j^{exp}) represents the estimated coordinates and true coordinates of the unknown nodes respectively. ALE is defined as the summation of LE of all unknown nodes to the total number of unknown nodes and computed as following:

$$ALE = \frac{\sum_{j=1}^{n} \sqrt{(x_j^{est} - x_j^{act})^2 + (y_j^{est} - y_j^{act})^2}}{n} \tag{26}$$

2) **Detection accuracy(ξ)**
The ratio of beacon nodes identified as malicious ($M_{identified}$) to the total number of malicious beacon nodes is known as and computed as following:

$$\xi = \frac{M_{identified}}{M_{Total}} \times 100 \tag{27}$$

3) **False-Positive rate (FPR)**
The ratio of number of trusty beacon nodes identified as malicious ($Trusty(M)_{identified}$) to the total number of trusty beacon nodes ($Benign_{Total}$) is recognized as FPR.

$$FPR = \frac{Trusty(M)_{identified}}{Trusty_{Total}} \tag{28}$$

4) **False-Negative Rate (FNR)**
The ratio of the number of malicious beacon nodes detected as trusty ($M(trusty)_{identified}$) to the total number of malicious nodes (M_{Total}).

$$FPR = \frac{M(trusty)_{identified}}{M_{Total}} \tag{29}$$

5) **Average Energy Consumption (AEC)**
AEC is the ratio of energy consumption during trust value evaluation (E_{trust}) to the total energy consumed for information transmission (E_{Tx}) and reception (E_{Rx}) and computed as following:

$$AEC = \frac{\sum_m E_{trust}}{\sum_m E_{Tx} + E_{Rx}} \tag{30}$$

B. PERFORMANCE EVALUATION

In this section, the simulated results of the proposed algorithm are compared with various existing algorithms. Firstly the impact of the ratio of beacon nodes on ALE is observed. For this simulation, 100 sensor nodes are deployed 5-30% beacon nodes with 5% malicious beacon nodes in a sensing area of $100 \times 100\ m^2$. In Table 3, the evaluated results are described by varying the ratio of beacon nodes. From the tabulated results, it is observed that the proposed algorithm performs 59.89%, 37.54% and 57.11% better as compared to B. B. Das et al., (2017) [18], T. Gaber et al. (2018) [17] and G. Han et al., (2016) [10] respectively.

Figure 7 illustrates the impact of ratio of malicious beacon nodes on ALE and reveals that as the malicious nodes increase the ALE for each algorithm also increases. It happens due to the fact that the unknown nodes can collect more erroneous information about beacon nodes caused inaccurate localization. The simulated results demonstrate

TABLE 3. Comparisons of ALE (m).

Ratio of beacon node	B. B. Das et al., (2017) [18]	T. Gaber et al. (2018) [17]	G. Han et al., (2016) [10]	Proposed algorithm
5	19.14	12.66	17.956	7.878
10	18.89	12.054	17.722	7.504
15	17.79	10.301	16.443	6.983
20	17.475	11.289	16.0114	6.794
25	17.012	10.698	14.901	6.489
30	16.64	10.0151	14.74	6.178
Average Error	**17.83**	**11.16**	**16.29**	**6.97**

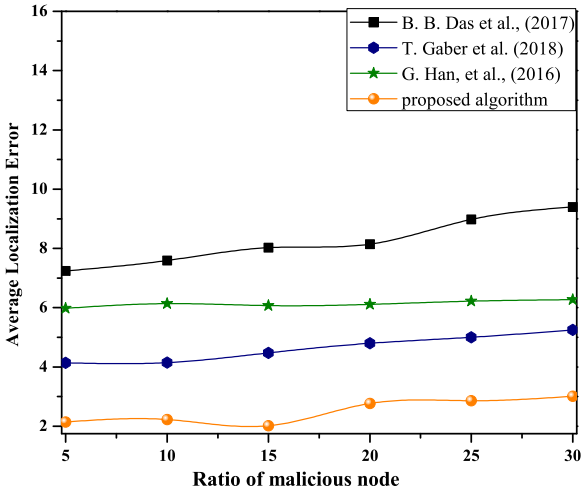

FIGURE 7. Impact of the ratio of malicious beacon node on ALE.

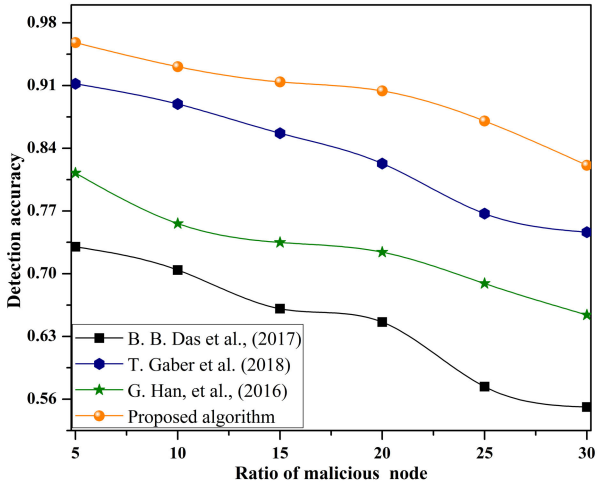

FIGURE 8. Impact of ratio of malicious beacon node on detection accuracy.

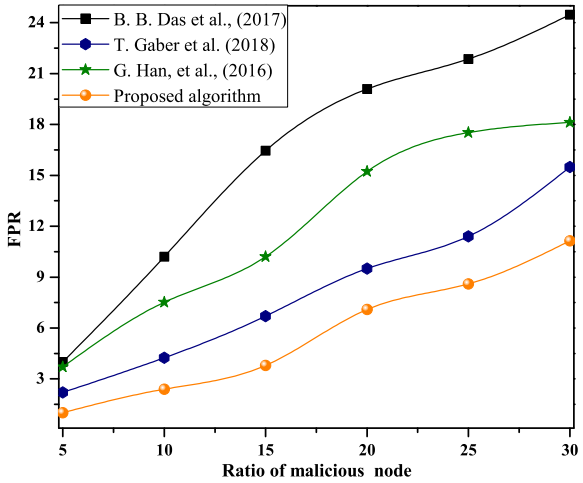

FIGURE 9. Impact of ratio of malicious beacon node on FPR.

that the proposed algorithm performs 69.1%, 46% and 59.12% better as compared to B. B. Das et al., (2017) [18], T. Gaber et al. (2018) [17] and G. Han et al., (2016) [10] respectively in the presence of malicious beacon nodes. The impact of ratio of malicious beacon nodes on detection accuracy is illustrated in Figure 8 and it can be observed that detection accuracy decreases as the number of malicious nodes increases because of false information collection in large amounts. The simulated results reveal that the proposed algorithm have 28.8%, 8.16% and 19.19% more detection accuracy as compared to B. B. Das et al., (2017) [18], T. Gaber et al. (2018) [17] and G. Han et al., (2016) [10] respectively. The impact of the ratio of malicious nodes on FPR and FNR is illustrated in Figure 9 and 10. The simulated results demonstrate that the proposed algorithm is significantly better in terms of FPR and FNR as compared to all existing algorithms. Figure 9 and 10 demonstrates that as the ratio of malicious nodes increases, the percentage of FPR and FNR also increases for all the algorithms. It happen due to the fact that large amounts of false information is collected as more number of malicious nodes presents in the network.

The proposed algorithm performs 64.95%, 31.27% and 52.94% better in terms of FPR as compared to B. B. Das et al., (2017) [18], T. Gaber et al. (2018) [17] and G. Han et al., (2016) [10] respectively. Also, the proposed algorithm achieves 60.53%, 23.22% and 50.45% better results in terms of FNR as compared to B. B. Das et al., (2017) [18], T. Gaber et al. (2018) [17] and G. Han et al., (2016) [10] respectively. In Figure 11 the impact of the ratio of beacon nodes on probability to find true location is illustrated. It shows that the probability of precise location increases as the number of beacon nodes increases in the network. It is examined from the simulated results that the proposed algorithm achieves 36%, 13.4% and 18.02%

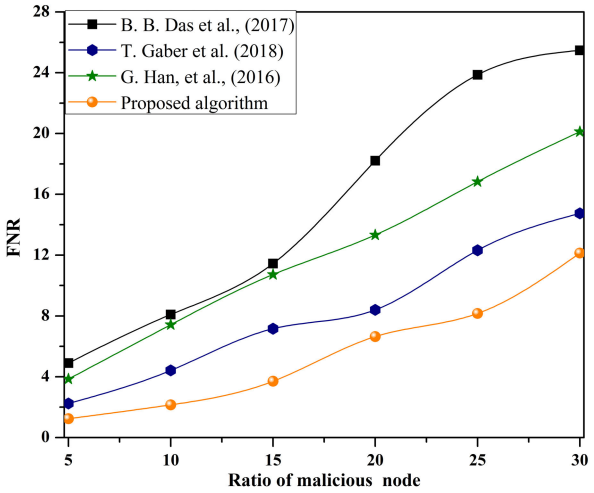

FIGURE 10. Impact of ratio of malicious beacon node on FNR.

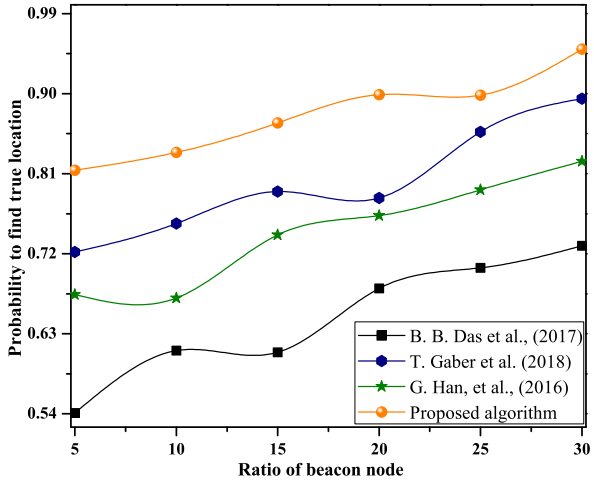

FIGURE 11. Impact of the ratio of beacon node on the probability of finding a true location.

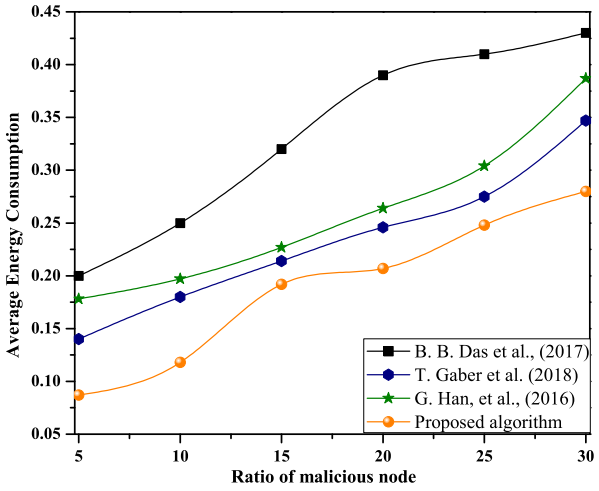

FIGURE 12. Impact of ratio of malicious node on AEC.

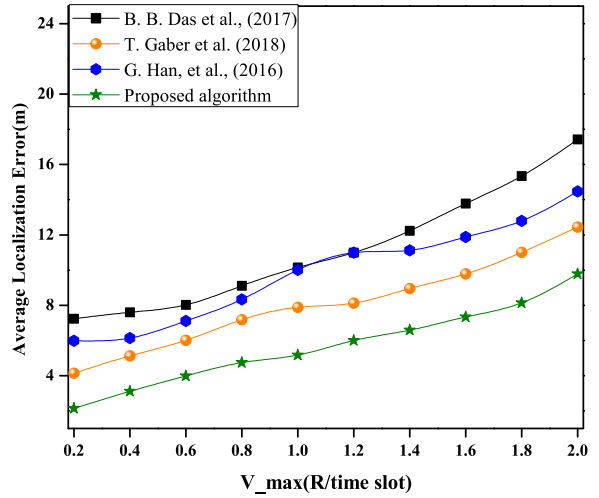

FIGURE 13. Impact of the mobility of nodes on ALE.

more accurate location of unknown nodes as compared to B. B. Das et al., (2017) [18], T. Gaber et al. (2018) [17] and G. Han et al., (2016) [10] respectively.

From the simulated results it is observed that the proposed algorithm is 43.03%, 19.33% and 26.56% more energy efficient as compared to B. B. Das et al., (2017) [18], T. Gaber et al. (2018) [17] and G. Han et al., (2016) [10] respectively. The average energy consumption of all algorithms is depicted in Figure 12. The proposed algorithm consumes less energy during trust value evaluation as the ratio of malicious beacon nodes increases in the network.

The impact of mobility on ALE is depicted in Figure 13. To perform the simulation, a total 100 sensor nodes are deployed with 30% benign/trusty nodes and 10% of total beacon nodes are malicious nodes with 40m communication radius. The mobility of each sensor node is randomly selected within a range from (0, $V\_(max.)$) and $V\_(max.)$ Is expressed in terms of R. Let us consider, $V\_(max.) = 20$, then $V\_(max.)$ is denoted as ($V\_(max.) = 0.5R$). From the simulated results demonstrated in Figure 13, it is observed that as the higher the mobility causes more localization error for all localization algorithms.

IV. CONCLUSION AND FUTURE SCOPE

The presented work successfully executes the trust evaluation process in decentralized blockchain generation of WSNs. Data-based trust evaluation reflects direct trust and indirect trust among participating beacon nodes which are key aspects of data trust. Further, the composite trust value of each beacon node is forwarded to BS to generate a decentralized blockchain-based trust management model. Moreover, only most trusty beacon nodes become the part of localization process for estimating the location of unknown nodes. Simulated results reveal that the proposed algorithm achieve 62.91%, 38.32% and 58.11% more accurate localization as compared to existing algorithms [10], [17], [18]. Moreover, it outperforms existing ones in terms of False

Positive Rate (FPR), False Negative Rate (FNR) and Average Energy Consumption (AEC). However, Bayesian statistics, Maximum likelihood estimation, reinforcement learning based trust evaluation and the complexity associated with the *length of blockchain* should be tested further to determine the completeness of the method.

REFERENCES

[1] S. Mukherjee and G. P. Biswas, "Networking for IoT and applications using existing communication technology," *Egyptian Informat. J.*, vol. 19, no. 2, pp. 107–127, 2018.

[2] T. Bala, V. Bhatia, S. Kumawat, and V. Jaglan, "A survey: Issues and challenges in wireless sensor network," *Int. J. Eng. Technol.*, vol. 7, nos. 2–4, p. 53, 2018.

[3] I. F. Akyildiz and M. C. Vuran, "WSN applications," in *Proc. Wireless Sensor Netw.*, 2011, pp. 17–35.

[4] M. P. Durisic, Z. Tafa, G. Dimic, and V. Milutinovic, "A survey of military applications of wireless sensor networks," in *Proc. Medit. Conf. Embedded Comput. (MECO)*, 2012, pp. 196–199.

[5] P. Pandey, "Study of WSNs: Its application and types," *Int. J. Sci. Res. Manage.*, vol. 3, no. 6, Jun. 2015. [Online]. Available: http://www.ijsrm.in/index.php/ijsrm/article/view/1139

[6] N. Patwari, J. N. Ash, S. Kyperountas, A. O. Hero, R. L. Moses, and N. S. Correal, "Locating the nodes: Cooperative localization in wireless sensor networks," *IEEE Signal Process. Mag.*, vol. 2, no. 4, pp. 54–69, Jul. 2005.

[7] Q. Zhang, J. Huang, J. Wang, C. Jin, J. Ye, and W. Zhang, "A new centralized localization algorithm for wireless sensor network," in *Proc. 3rd Int. Conf. Commun. Netw. China*, Hangzhou, China, Aug. 2008, pp. 625–629.

[8] D. Dragoş, D. Niculescu, and B. Nath, "DV based positioning in ad hoc networks," *Telecommun. Syst.*, Jan. 2003, nos. 1–4, pp. 267–280, Jan. 2003.

[9] Y. Zhang, W. Liu, and Y. Fang, "Secure localization in wireless sensor networks," in *Proc. IEEE Mil. Commun. Conf. MILCOM*, Oct. 2005, pp. 3169–3175.

[10] G. Han, L. Liu, J. Jiang, L. Shu, and J. J. P. C. Rodrigues, "A collaborative secure localization algorithm based on trust model in underwater wireless sensor networks," *Sensors*, vol. 16, no. 2, p. 229, 2016.

[11] Y. Yin, W. Xu, Y. Xu, H. Li, and L. Yu, "Collaborative QoS prediction for mobile service with data filtering and slopeone model," *Mobile Inf. Syst.*, vol. 2017, pp. 1–14, Jun. 2017.

[12] Y. Yin, Y. Xu, W. Xu, M. Gao, L. Yu, and Y. Pei, "Collaborative service selection via ensemble learning in mixed mobile network environments," *Entropy*, vol. 19, no. 7, p. 358, 2017.

[13] T. Zhang, J. He, and Y. Zhang, "Trust based secure localization in wireless sensor networks," in *Proc. Int. Symp. Intell. Inf. Process. Trusted Comput., (IPTC)*, Oct. 2011, pp. 55–58.

[14] N. Yu, L. Zhang, and Y. Ren, "BRS-based robust secure localization algorithm for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 3, 2013, Art. no. 107024.

[15] K. Saini and P. Ahlawat, "A trust-based secure hybrid framework for routing in WSN," *Adv. Intell. Syst. Comput.*, vol. 707, pp. 585–591, Nov. 2018.

[16] D. Jayashree, V. U. Rani, and K. S. Sundaram, "Trust based misbehavior detection in wireless sensor networks," *Appl. Mech. Mater.*, vol. 622, pp. 191–198, Aug. 2014.

[17] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, "Trust-based secure clustering in WSN-based intelligent transportation systems," *Comput. Netw.*, vol. 146, pp. 151–158, Dec. 2018.

[18] B. B. Das and S. K. Ram, "Localization using beacon in wireless sensor networks to detect faulty nodes and accuracy improvement through DV-Hop algorithm," in *Proc. Int. Conf. Inventive Comput. Technol., (ICICT)*, vol. 1, Aug. 2016, pp. 1–5.

[19] G. D. Devanagavi, N. Nalini, and R. C. Biradar, "Trusted neighbors based secured routing scheme in wireless sensor networks using agents," *Wireless Pers. Commun.*, vol. 78, no. 1, pp. 1–28, 2014.

[20] G. Kumar, M. K. Rai, H. Kim, and R. Saha, "A secure localization approach using mutual authentication and insider node validation in wireless sensor networks," *Mobile Inf. Syst.*, vol. 2017, Nov. 2017, Art. no. 3243570.

[21] G. Kumar, M. K. Rai, and R. Saha, "Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in Wireless Sensor Networks," *J. Netw. Comput. Appl.*, vol. 99, pp. 10–16, Dec. 2017.

[22] P. Amish and V. B. Vaghela, "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol," *Procedia Comput. Sci.*, vol. 79, pp. 700–707, 2016.

[23] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, and P. Kar, "Wormhole detection based on ordinal MDS Using RTT in wireless sensor network," *J. Comput. Netw. Commun.*, vol. 2016, Oct. 2016, Art. no. 3405264.

[24] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2018.

[25] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[26] E. F. Jesus, V. R. Chicarino, C. V. de Albuquerque, and A. A. D. A. Rocha, "A survey of how to use blockchain to secure Internet of Things and the stalker attack," *Secur. Commun. Netw.*, vol. 2018, no. 1, pp. 1–27, 2018, Art. no. 9675050.

[27] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[28] A. Lei, Y. Cao, S. Bao, D. Li, P. Asuquo, H. Cruickshank, and Z. Sun, "A blockchain based certificate revocation scheme for vehicular communication systems," *Future Gener. Comput. Syst.*, to be published.

[29] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," *Future Gener. Comput. Syst.*, vol. 92, pp. 357–373, Mar. 2019.

[30] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Inf. Syst.*, vol. 2018, pp. 1–10, Aug. 2018, Art. no. 6874158.

[31] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, p. 970, 2019.

[32] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. (Trustcom/BigDataSE)*, Aug. 2018, pp. 98–103.

[33] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[34] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.

[35] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6835–6842, Aug. 2019.

[36] E. Mohamed, H. Zakaria, and M. B. Abdelhalim, "An improved DV-HOP localization algorithm," in *Proc. Adv. Intell. Syst. Comput.*, vol. 533, 2017, pp. 332–341, doi: 10.1007/978-3-319-99010-1.

TAI-HOON KIM received the B.E. and M.E. degrees from Sungkyunkwan University, South Korea, and the Ph.D. degrees from the University of Bristol, U.K., and the University of Tasmania, Australia. He is currently with Beijing Jiotong University, Beijing, China. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.

REKHA GOYAT received the M.Tech. degree from the Department of Electronics and Communication Engineering, Punjab Technical University, Punjab, India, in 2015. She is currently pursuing the Ph.D. degree with the Department of Electronics and Communication Engineering, Lovely Professional University, Punjab. She has published ten research articles in international journals. Her research areas are wireless sensor networks, localization, and network security.

MRITUNJAY KUMAR RAI received the M.E. degree in digital system from the Motilal Nehru National Institute of Technology, Allahabad, India, and the Ph.D. degree from the ABV Indian Institute of Information Technology and Management, Gwalior, India. He worked as an Associate Professor with Lovely Professional University, Phagwara, India. He is currently with Lovely Professional University, Phagwara, India. He has published more than 40 research articles in reputed international conferences and international journals. His research interests include wireless networks, network security, and cognitive radio Networks.

GULSHAN KUMAR received the B.Tech. degree in computer science engineering from the Amritsar College of Engineering, Amritsar, in 2009, the M.Tech. and Ph.D. degrees from Lovely Professional University, Punjab, India, with area of specialization in position and location computation in wireless sensor networks. He is currently working as an Associate Professor with Lovely Professional University, Punjab. He has many publications in well-renowned International journals and Conferences.

WILLIAM J. BUCHANAN is currently a Professor of cryptography, and was awarded an OBE for his services to Cybersecurity, in 2017. He also leads the Blockpass ID Lab, Edinburgh Napier University. He has authored 30 academic books and over 250 research articles. His main research interests include distributed ledger technology, identity systems, trust-based infrastructures, and cryptography. Along with this his work has supported the creation of a number of spin-out companies and international patents.

RAHUL SAHA received the B.Tech. degree in computer science engineering from the Academy of Technology, West Bengal, and the M.Tech. and Ph.D. degrees from Lovely Professional University, Punjab, India, with area of specialization in cryptography, position, and location computation in wireless sensor networks. He is currently working as an Associate Professor with Lovely Professional University. He has many publications in well-renowned international journals and conferences.

REJI THOMAS received the Ph.D. degree from IIT Delhi. He is currently a Professor with Lovely Professional University, Phagwara, Punjab, India. His research interests include logic, memory, and energy storage devices.