Hindawi
Journal of Computer Networks and Communications
Volume 2019, Article ID 2054298, 13 pages
https://doi.org/10.1155/2019/2054298

Research Article

LB-IDS: Securing Wireless Sensor Network Using Protocol Layer Trust-Based Intrusion Detection System

Umashankar Ghugar,[1] Jayaram Pradhan,[1] Sourav Kumar Bhoi ,[2] and Rashmi Ranjan Sahoo[2]

[1]*Department of Computer Science, Berhampur University, Odisha 760007, India*
[2]*Advanced Computing and Research Lab, Department of Computer Science and Engineering, Parala Maharaja Engineering College, Berhampur 761003, Odisha, India*

Correspondence should be addressed to Sourav Kumar Bhoi; souravbhoi@gmail.com

Received 31 August 2018; Accepted 4 December 2018; Published 6 January 2019

Academic Editor: Peter Mueller

Wireless sensor network (WSN) faces severe security problems due to wireless communication between the nodes and open deployment of the nodes. The attacker disrupts the security parameters by launching attacks at different layers of the WSN. In this paper, a protocol layer trust-based intrusion detection system (LB-IDS) is proposed to secure the WSN by detecting the attackers at different layers. The trust value of a sensor node is calculated using the deviation of trust metrics at each layer with respect to the attacks. Mainly, we consider trustworthiness in the three layers such as physical layer trust, media access control (MAC) layer trust, and network layer trust. The trust of a sensor node at a particular layer is calculated by taking key trust metrics of that layer. Finally, the overall trust value of the sensor node is estimated by combining the individual trust values of each layer. By applying the trust threshold, a sensor node is detected as trusted or malicious. The performance of LB-IDS is evaluated by comparing the results of the three performance parameters such as detection accuracy, false-positive rate, and false-negative rate, with the results of Wang's scheme. We have implemented jamming attack at the physical layer, back-off manipulation attack at the MAC layer, and sinkhole attack at the network layer using simulations. We have also implemented a cross-layer attack using the simulation where an attacker simultaneously attacks the MAC layer and network layer. Simulation results show that the proposed LB-IDS performs better as compared with Wang's scheme.

1. Introduction

WSN is widely used in many applications such as industrial monitoring, environmental monitoring, forest monitoring, health care, and military. The architecture of WSN is categorized into clustered and flat [1]. In the flat architecture, the sensor nodes (SNs) communicate with the base station (BS) directly or by relaying the data through other nodes. When a WSN is clustered, the SNs are arranged within a specific area by forming a cluster. One node acts as a cluster head (CH) to control the whole communication between the nodes. The SNs communicate with the BS through the CHs. An SN exchange its information by forwarding the data to its CH, and then the CH sends the data directly to the BS or relaying the data through the CHs. Clustering is an important mechanism in WSN for many advantages such as energy efficiency, reduction in communication overhead, delay minimization, better communication, and topology management.

Security in WSN is a major issue during the past decade due to open deployment of SNs and wireless communications between them [2–4]. The attacker disrupts the security attributes by launching attacks at different layers. At the physical layer, a malicious node can be attacked by denial of service (DoS) attack by jamming the physical channel [5–9]. In this attack, an attacker continuously interferes with the frequencies used for communication by broadcasting unnecessary signals. These signals jam the network, and a genuine node denies to give services because it is busy in receiving the signals. The codes in the SN can also be modified, and the node can be tampered or replaced with an untrusted node [1, 7]. At the MAC layer [10, 11], the attacker disrupts the network availability by obtaining unfair channel priority, collisions, etc. The MAC layer include many types of attack such as back-off manipulation attack, RTS/CTS frame modification, guaranteed time slot attack, and collisions. At the network layer [12–14], the attacker attacks by disrupting the routing of data from source to the destination by acquiring control on the data. The attacker attacks using selective forwarding attack, sinkhole attack, wormhole attack, black hole attack, sybil attack, etc. Apart from the single protocol layer attack, there is another type of attack called as cross-layer attack where multiple layers are attacked [15–17]. IDS plays an essential role in securing the WSN as a second wall, where it detects the misbehavior of the nodes that violates the security mechanisms [18–23]. In WSN, it is difficult to use complex security mechanisms because it increases the energy consumption of a SN. Therefore, WSNs are applying light-weight security mechanisms for protecting the network [24, 25], and IDS is providing a platform by recording the misbehavior of the SNs and reporting it to the administrator for taking countermeasures.

IDS is mainly divided into anomaly detection and misuse detection [26, 27]. In misuse detection, there is prior knowledge about the attacks, and it is easy to detect the attacks. However, it is difficult to detect the unknown attacks. Unknown attacks are detected using anomaly detection. Anomaly detection compares the current operations of a node with the behavior and status of a normal node to check the misbehavior. In this paper, we have mainly focused on the anomaly detection system (IDS). However, many IDS schemes only work on particular type of attacks based on a single layer. It is needed to identify the cross-layer attack where an attacker attacks multiple layers at a time. It is difficult to identify such type of attacks because the attacker has different behavior at a time. To improve the detection of such attacks, the trust metrics are selected at each protocol layer, and the parameters have a high impact on the performance of the IDS.

We are mainly motivated from the method proposed by Wang et al. [1]. The authors proposed an IDS for WSN using trust-based system. In this model, a trust is separately calculated for each SN at the physical layer, MAC layer, and network layer using trust metrics. Finally, each layer trust is combined to form a single overall trust value. This trust value is called as the direct trust value of node *A* on node *B*, where node *A* is the evaluator node or monitoring node. In this model, the monitoring node calculates the trust value of the monitored node by using the direct experience with the monitored node (according to the trust metrics). This may reduce the performance of the system by reducing the detection accuracy (DA) and increasing the false-positive rate (FPR) and false-negative rate (FNR). However, in our model, we have calculated the trust value of the monitored node by taking direct experience and the experiences of other nodes (neighbor nodes) with the monitored node. This increases the DA and reduces FPR. If the trust value of a monitored node is higher than a threshold, then the node is treated as a reliable or genuine node. The main motivation is also elaborated with respect to the three layers as follows. In [1], at the physical layer, energy consumption is considered as the trust metric for the trust value calculation. As jamming attack is considered, a node that jams the network has high energy consumption due to continuous signal generation. However, if a genuine node in the communication range has performed communication for a longer time, then it has a low energy, and this node is considered as a malicious node [1]. Therefore, we have calculated the trust using the direct experience and experiences (signal reception) of other neighbor nodes with the monitored node. At the MAC layer, back-off time is considered as the trust metric for the trust value calculation. As back-off manipulation attack is considered, a node that has less back-off time will get higher access to the channel for communication. However, if a genuine node in the communication range sends more messages for communication, then this node is considered as a malicious node [1], because it is getting more channel priority. Therefore, we have calculated the trust using the direct experience and experiences (channel priority) of other neighbor nodes with the monitored node. At the network layer, the number of hops advertised is considered as the trust metric for the trust value calculation. As sinkhole attack is considered, a node that broadcasts less number of hops is considered as a malicious node. However, if a genuine node in the communication range has less number of hops, then this node is considered as a malicious node [1]. Therefore, we have calculated the trust by using the direct experience and experiences (hop count advertisement) of neighbor nodes with the monitored node. This increases the DA and reduces the FPR. This scheme is applicable for clustered and flat networks. The main contributions of this paper are stated as follows:

(1) LB-IDS is proposed to detect the malicious nodes in the clustered WSN. In this method, a trust value of an SN is individually calculated at the physical layer, MAC layer, and network layer using the deviation of trust metrics. The deviation is calculated from the direct experience and experiences of the neighbor nodes with the monitored node.

(2) The monitoring node or evaluator node estimates the trust value of the monitored node using the deviation factor. Then, the individual trust values of each layer are combined to calculate the overall trust value of an SN. Then, the trust value is transferred to the CH. Then, the CH decides whether the SN is genuine or malicious using a threshold value. This trust value is updated at regular intervals.

(3) The analysis of LB-IDS is performed in terms of message complexity, memory overhead, energy consumption, and trust evaluation.

(4) Simulation results show that LB-IDS performs better than the model by Wang et al. [1] in terms of DA, FPR, and FAR. The performance is analyzed by considering the jamming attack in the physical layer, back-off manipulation attack in the MAC layer, and

sinkhole attack in the network layer, and finally cross-layer attack is also implemented at the network layer and MAC layer.

The remaining portion of the paper is organized as follows. Section 2 presents the work done in the field of trust-based security in WSN. Section 3 describes the proposed LB-IDS model. Section 4 presents the trust estimation at each layer. Section 5 presents the analysis of the LB-IDS. Section 6 presents the results and discussion. At last, the conclusion and future work is presented in Section 7.

2. Related Works

Securing wireless sensor network using trust-based schemes are very effective methods for supporting WSN against the security threats and vulnerabilities. Many research works are performed to secure the network using the trust-based models [28–33]. The trust-based models mainly use fuzzy models, probability models, statistical methods, weighting methods, etc. LB-IDS mainly focuses on the statistical method where it uses the average and deviation of trust metrics to detect an attack in a layer.

In [25, 34, 35], to determine the trust degree, the authors have used the fuzzy theory concept in the network. Feng et al. [34] proposed a trust evaluation algorithm (NBBTE) based on banding belief theory. In this scheme, a node finds the trust value of its neighboring node using the direct and indirect trust based on many trust factors. Then, fuzzy model is used to know the level of trustworthiness of each neighbor node. Then, DS evidence theory is used to aggregate the trust values to find a final trust level of a node. Wu et al. [35] proposed a trust model for securing WSN using fuzzy model and evidence model. Fuzzy set theory is used for finding trust level of the sensors, and evidence theory is used for aggregating the trust value. Shao et al. [25] proposed a trust model for WSN where the trust recommendations provided by the sensors are evaluated using fuzzy model. In [36, 37], the authors calculated the trust value of a sensor node using probability distribution method. Ganeriwal et al. [36] proposed a method that is based on distributed reputation framework. It uses watchdog technique to observe behaviors of nodes. Luo et al. [37] used identity labels for the sensor nodes to design a dynamic trust management scheme. In [24, 38–42], the authors used the weighting method for trust calculation and evaluation. Atakli et al. [38] used weighting method to detect malicious activity in the network by maintaining the hierarchy and continuous monitoring. Shaikh et al. [41] detected the malicious nodes in a clustered network by finding group trust for a node. Yao et al. [42] proposed a parameter and localized based trust management scheme to provide security to WSN. Li et al. [24] proposed a simple and dependable trust model for clustered environment of WSN. Jiang et al. [40] used direct as well as indirect trust for trust calculation of a sensor node in WSN. Direct trust calculation includes energy, data, and communication trusts. Indirect trust calculation includes the recommendations from the neighbor nodes for the monitored node. Ishmanov et al. [43] measured the weightage of misbehavior of a node for the detection of malicious nodes in the network. Bao et al. [44, 45] proposed a trust model for WSN using weighting parameters and reduced the false-positive rate using statistical methods. Zhang et al. [46] proposed a trust model based on cloud model for clustered WSN. Rajeshkumar et al. [47] proposed an adaptive trust-based acknowledgment IDS using active successful deliveries. In this method, Kalman filter is used to estimate the trust factor of a node. In [48], we have proposed a physical layer IDS to provide security at the physical layer. This method only detects the denial of service attack due to jamming attack. It lacks security at MAC layer and network layer.

From the literature discussed above, it is observed that selecting proper trust metrics to calculate the trust of an SN is very essential. Therefore, to design an IDS, the behavior of the nodes should be monitored. In this work, we have selected the proper trust metrics at each layer for trust calculation and detected the behavior of a node according to the attack. To the best of our knowledge, very less work has been done in this area to design a protocol layer trust-based IDS. In this paper, the trust is calculated at each layer by considering the deviation of trust metrics. Then, the overall trustworthiness of a sensor node is estimated by combining the individual trust values.

3. System Model

The system model describes about the topology and communication, and also about the attack models used in this work.

3.1. Network Model. The network model consists of a WSN that is clustered. A cluster in the network has a CH and SNs. The SNs communicate with each other using wireless communication. The SNs can directly communicate with the base station (BS) using wireless communication or indirectly through other SNs. The CHs can communicate with each other using wireless communication. The CH has high processing and high computing capability. It is assumed that the CH has high battery power. In this model, an SN evaluates its neighbor using the LB-IDS model. Then, the trust value is periodically transferred to the CH. The trust is periodically updated at the CH in Δt time. Here, each node applies the watchdog technique, where a node monitors its neighbor nodes continuously by updating the trust value. Figure 1 shows the clustered WSN framework. The individual trust is calculated at each layer, and it is finally aggregated to generate the overall trust of an SN. The trust metrics are considered as the behavior of the nodes at each layer. These parameters are used for trust calculation at each layer.

The model for LB-IDS is shown in Figure 2, and the notations used in this paper are presented in Table 1. In this model, an SN monitors its neighbor node by estimating the trust value at each layer such as physical layer, MAC layer, and network layer. Most of the attacks are mainly on the network layer because this layer is mainly used for routing the data in the network [1]. Therefore, we have only

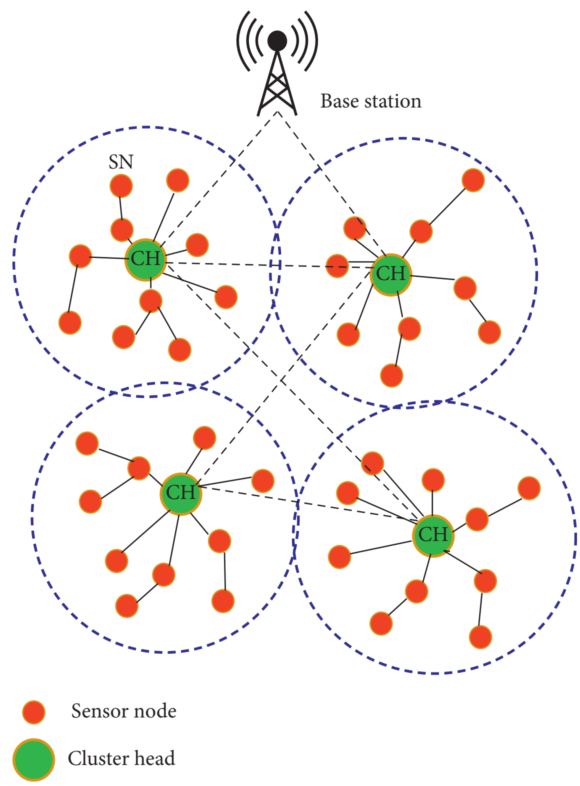

Figure 1: A wireless sensor network with CHs, BS, and SNs.

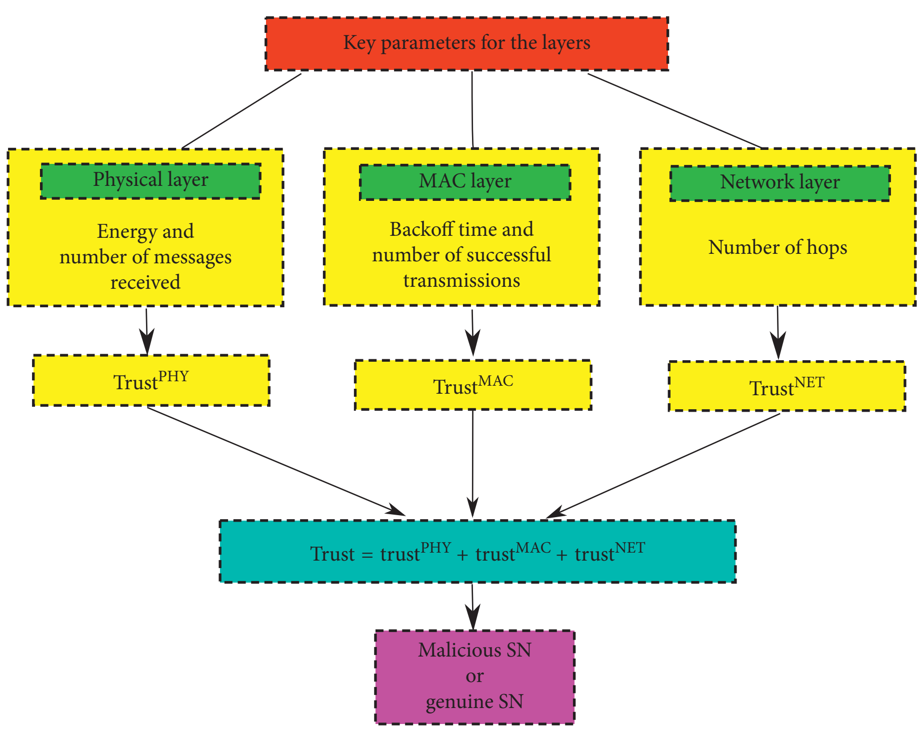

Figure 2: LB-IDS for clustered WSN.

considered these three layers to estimate final trustworthiness of an SN [1, 48]. Firstly, the trust metrics are chosen to calculate trust at each layer. The trust metrics at the physical layer are energy consumption of an SN and the number of messages received from the SN. The trust metrics at the MAC layer are back-off time and the number of successful transmission. The trust metrics at the network layer is the number of hops advertised. In the later sections, we have

Table 1: Notation and description.

Notations	Description
SN	Sensor node
CH	Cluster head
$T_{jk}(t)$	Trust value
Λ	Weight factor for overall trust calculation
t	Time
μ	Weight factor for updating trust
Nmr	Number of messages received
Ecm	Energy consumed
Nst	Number of successful transmissions
Bt	Back-off time
hp	Hop count
Dv	Relative deviation
Rec	Recommendation
α	Weight factor for T_{jk}^{PHY} calculation
β	Weight factor for T_{jk}^{MAC} calculation

justified why these parameters are considered for individual trust calculation at each layer. The overall trust of an SN is calculated by aggregating all individual trusts of each layer. Then, the overall trust value of the SN is forwarded to the CH. The CH finds whether the SN is malicious or genuine using the thresholding scheme.

Let $T_{jk}(t)$ is the overall trust value of node k at time t, calculated by node j. This is represented as follows:

$$T_{jk}(t) = \lambda_1 \times T_{jk}^{\mathrm{PHY}}(t) + \lambda_2 \times T_{jk}^{\mathrm{MAC}}(t) + \lambda_3 \times T_{jk}^{\mathrm{NET}}(t), \quad (1)$$

where $T_{jk}^{\mathrm{PHY}}(t)$ is the trust calculated at the physical layer (PHY) by considering the deviation, $T_{jk}^{\mathrm{MAC}}(t)$ is the trust calculated at the MAC layer (MAC) by considering the deviation, and $T_{jk}^{\mathrm{NET}}(t)$ is the trust calculated at the network layer (NET) by considering the deviation. The sum of the weight parameters λ_1, λ_2, and λ_3 are 1 ($\lambda_1 + \lambda_2 + \lambda_3 = 1$). The value of individual weight $\lambda \epsilon [0, 1]$. The values of the weights are decided according to the IDS, i.e., whenever there is attack at the physical layer, the λ_1 will be considered by the IDS as 1 and the rest of λ_2 and λ_3 are considered as 0. However, at the time of cross-layer attack between the MAC layer and network layer, λ_2 and λ_3 values are given equal weights and λ_1 is considered as 0. To reduce the complexity of the network, we have chosen parameters according to the requirement. We have considered the minimum number of parameters that are mostly suitable to detect the attacks at each layer. The trustworthiness of a node is updated periodically after a Δt time:

$$T_{jk}(t) = \mu \times T_{jk}(t - \Delta t) + (1 - \mu) \times T_{jk}(t), \quad (2)$$

where $T_{jk}(t - \Delta t)$ represents the past trust value of node j on node k. The weight value $\mu\, \epsilon$ varies between 0 and 1. The value of μ depends on the IDS. This weight factor describes the priority of previous trust value and current trust value to generate the new trust value for a node. From equation (2), it is observed that the past experience is also considered because the overall trust should take the previous and current trust values. In the next section, we have computed the trust values at each layer.

3.2. Attack Model. In the attack model, we have discussed those attacks that are used for evaluating the performance of LB-IDS. The attacks are described with respect to each layer such as physical layer, MAC layer, and network layer.

3.2.1. Attack at the Physical Layer. At the physical layer, jamming a network is a common security problem where a malicious node continuously transmits short range signals. These signal transmission create traffic in the network. Due to this traffic, a genuine node remains busy in receiving the unnecessary signals and denies other applications. This is called as denial of service (DoS). The attack model can be represented mathematically as follows:

$$i = e + m, \quad (3)$$

where i is the information that may be correct or incorrect depending on the IDS, e denotes the information expected, and m denotes the information which has malicious content. In this layer, energy consumption (Ecm) and the number of messages received (Nmr) are considered as the i to detect the malicious nodes in the network. Figure 3 shows the jamming attack where the malicious node k sends continuous signal to the genuine node j. In this model, we assume that the number of messages (nm) generated for a genuine node in a particular time interval is smaller than the number of messages generated by a malicious node (nm$'$), where nm$'$ > nm. In this model, the number of messages generated follows the pseudorandom number uniform distribution pattern.

3.2.2. Attack at the MAC Layer. At the MAC layer, getting a channel priority is a major factor. Therefore, we have considered back-off manipulation attack where the malicious node attacks the system by modifying the back-off time. Here, back-off time is random in nature. It is manipulated by lowering the back-off time, so that the priority of getting the channel access increases. This increases the number of successful transmissions (Nst). In this layer, back-off time (Bt) parameter and the number of successful message transmission (Nst) parameter are considered as i to detect the malicious nodes in the network. Figure 4 shows the back-off time manipulation attack where the malicious node k sends continuous signal to the genuine node j by getting the channel priority in less time.

3.2.3. Attack at the Network Layer. At the network layer, routing information is mainly affected by the attackers by advertising incorrect information in the network like the minimum hop count. In this work, we have considered the sinkhole attack. In this attack, the malicious node send regular updates by advertising bogus routing information like low hop count. From Figure 5, it is observed that the malicious node 2 advertises minimum hop count to the destination (to the source node 1). The node 1 then forwards the data in the direction of node 2. The data may

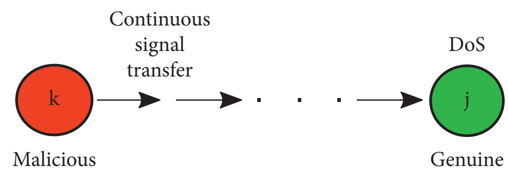

Figure 3: Jamming attack at the physical layer.

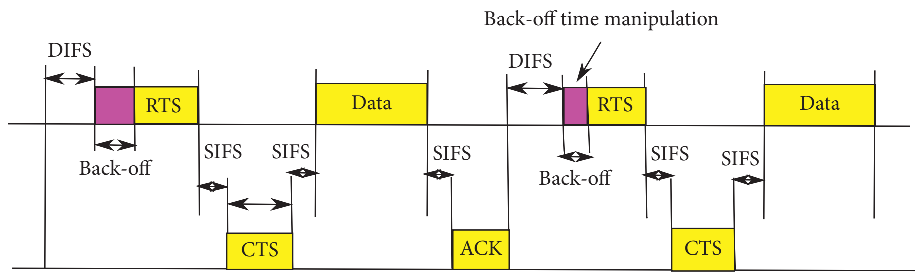

Figure 4: Back-off manipulation attack at the MAC layer.

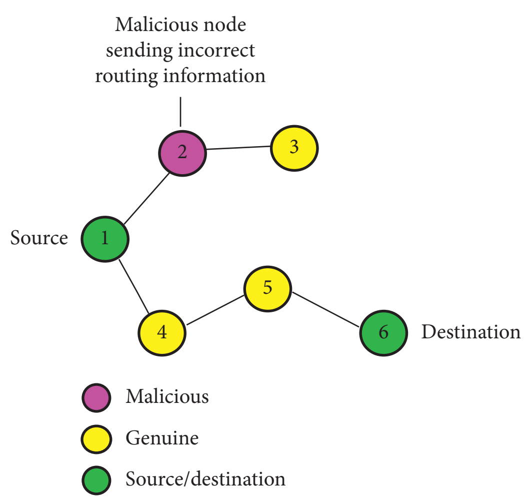

Figure 5: Sinkhole attack at the network layer.

be selectively forwarded to the next node or all packets are dropped. We assume that the node advertises the low hop count information in the route reply packet (RREP) during route discovery in Ad hoc On Demand Distance Vector routing protocol (AODV) [1]. Therefore, the sinkhole attack needs to be detected. In this layer, hop count (hp) parameter is considered as i to detect the malicious nodes in the network.

3.2.4. Cross-Layer Attack. In cross-layer attack, a malicious node in the network attacks two or more layers at a time. In this model, we have considered the back-off manipulation attack and sinkhole attack at the MAC layer and network layer, respectively. The attacker gets high priority of accessing the channel and advertises minimum hop count information. This attack should also be detected by the LB-IDS. Figure 6 shows the cross-layer attack by the malicious node k on the MAC layer and network layer.

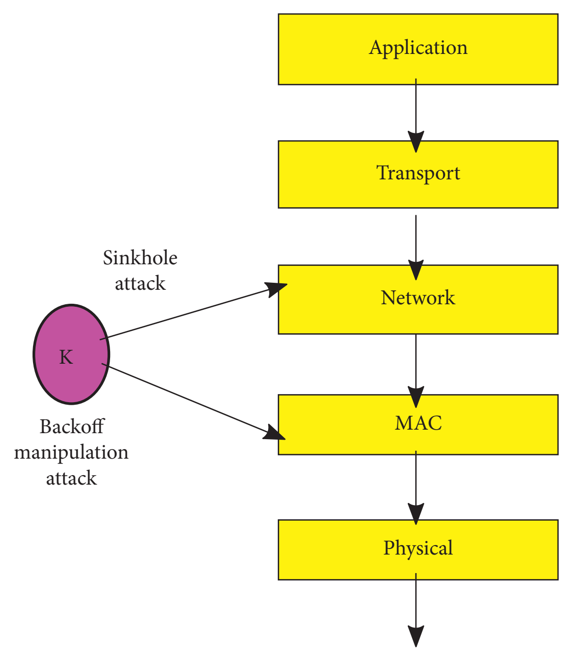

Figure 6: Cross-layer attack at the protocol layer.

4. Estimation of Trust

In this section, we have estimated the trust at the physical layer, MAC layer, and network layer.

4.1. Estimation of Physical Layer Trust. At the physical layer, Ecm and Nmr are considered as the trust metrics to calculate the deviations. The physical layer of the protocol layer represents the transmission of bits and receiving of bits [48]. Therefore, energy consumption is a trust metric for the transmission of or receiving a message of length l_M bits. According to the jamming attack at the physical layer, an attacker continuously transmits signals or packets, due to which energy consumption occurs. Therefore, Ecm and Nmr are considered as the trust metrics for trust estimation at the physical layer. Here, the monitoring node j collects recommendations from its neighbor nodes after the time period Δt. These recommendations are the Ecm and Nmr values generated by direct experience of the neighbor nodes with monitored node k. The average of the recommendations (Ecm and Nmr) are calculated as follows:

$$\overline{\mathrm{Rec}_{\mathrm{Ecm}}} = \frac{1}{n}\sum_{i=1}^{n} \mathrm{Ecm}_n,$$
$$\overline{\mathrm{Rec}_{\mathrm{Nmr}}} = \frac{1}{n}\sum_{i=1}^{n} \mathrm{Nmr}_n, \tag{4}$$

where $\overline{\mathrm{Rec}_{\mathrm{Ecm}}}$ and $\overline{\mathrm{Rec}_{\mathrm{Nmr}}}$ are the average of the recommendations collected after Δt time, respectively, and n is the number of neighbor nodes. The Ecm provided by the neighbor node to the monitoring node j is computed by the energy consumed in transmission during the Δt time and it is represented as follows [49]:

$$\mathrm{Ecm}_{\mathrm{bit}} = \mathrm{current} \times \mathrm{voltage} \times \mathrm{time},$$
$$\mathrm{Ecm}_{N_t} = N_t \times l_M \times \mathrm{Ecm}_{\mathrm{bit}}, \tag{5}$$

where N_t is the number of messages transmitted by node k to the neighbor node. From N_t, we can know the number of messages received Nmr at the neighbor node.

After calculation of $\overline{\mathrm{Rec}_{\mathrm{Ecm}}}$ and $\overline{\mathrm{Rec}_{\mathrm{Nmr}}}$, the relative deviation of the trust metrics of node k (monitored node) are represented as follows:

$$\mathrm{Dv}_{\mathrm{Ecm}} = \frac{\Delta \mathrm{Ecm}_k(t) - \overline{\Delta \mathrm{Rec}_{\mathrm{Ecm}}(t)}}{\overline{\Delta \mathrm{Rec}_{\mathrm{Ecm}}(t)}},$$
$$\mathrm{Dv}_{\mathrm{Nmr}} = \frac{\Delta \mathrm{Nmr}_k(t) - \overline{\Delta \mathrm{Rec}_{\mathrm{Nmr}}(t)}}{\overline{\Delta \mathrm{Rec}_{\mathrm{Nmr}}(t)}}, \tag{6}$$

where $\mathrm{Dv}_{\mathrm{Ecm}}$ and $\mathrm{Dv}_{\mathrm{Nmr}}$ are the deviations of trust metrics, respectively. $\Delta \mathrm{Ecm}_k(t)$ is $\mathrm{Ecm}_k(t-\Delta t) - \mathrm{Ecm}_k(t)$ and $\Delta \mathrm{Nmr}_k(t)$ is $\mathrm{Nmr}_k(t-\Delta t) - \mathrm{Nmr}_k(t)$. $\mathrm{Ecm}_k(t)$ denotes the energy consumed at time t and $\Delta \mathrm{Ecm}_k(t)$ is the energy consumed during Δt time (between node j and node k).

Now, we calculate the individual trust using the Ecm and Nmr parameters as follows:

$$T_{jk}^{\mathrm{Ecm}}(t) = \begin{cases} 1 - \mathrm{Dv}_{\mathrm{Ecm}}(t), & \text{if } \Delta \mathrm{Ecm}_k(t) > \overline{\Delta \mathrm{Rec}_{\mathrm{Ecm}}(t)}, \\ 1, & \text{else}, \end{cases} \tag{7}$$

$$T_{jk}^{\mathrm{Nmr}}(t) = \begin{cases} 1 - \mathrm{Dv}_{\mathrm{Nmr}}(t), & \text{if } \Delta \mathrm{Nmr}_k(t) > \overline{\Delta \mathrm{Rec}_{\mathrm{Nmr}}(t)}, \\ 1, & \text{else}. \end{cases} \tag{8}$$

From equations (7) and (8), it is observed that if $\Delta \mathrm{Ecm}_k(t)$ and $\Delta \mathrm{Nmr}_k(t)$ are greater than the average values, then the trustworthiness of the node reduces. The final trust at the physical layer is calculated as follows:

$$T_{jk}^{\mathrm{PHY}}(t) = \alpha_1 \times T_{jk}^{\mathrm{Ecm}}(t) + \alpha_2 \times T_{jk}^{\mathrm{Nmr}}(t), \tag{9}$$

where α_1 and α_2 belong to [0, 1] and the sum is 1 ($\alpha_1 + \alpha_2 = 1$). The values of α_1 and α_2 depend on the IDS system.

4.2. Estimation of MAC Layer Trust.

At the MAC layer, back-off time Bt and the number of successful message transmission Nst are considered as the trust metrics to calculate the deviations. The MAC layer of the protocol layer is mainly used for accessing the channel. Therefore, back-off time is a trust metric for the successful transmission of a message. According to the back-off manipulation attack in the MAC layer, a malicious node shortens the back-off time to get quicker channel access. Then, it successfully transmits the messages to the neighbor nodes with a high channel priority. Therefore, Bt and Nst are considered as the trust metrics for trust estimation at the MAC layer. Here, the monitoring node j collects recommendations from its neighbor nodes after the time period Δt. These recommendations are the Bt and Nst values generated by direct experience of the neighbor nodes with monitored node k. The average of the recommendations (Bt and Nst) are calculated as follows:

$$\overline{\mathrm{Rec}_{\mathrm{Bt}}} = \frac{1}{n}\sum_{i=1}^{n} \mathrm{Bt}_n,$$
$$\overline{\mathrm{Rec}_{\mathrm{Nst}}} = \frac{1}{n}\sum_{i=1}^{n} \mathrm{Nst}_n, \tag{10}$$

where $\overline{\mathrm{Rec}_{\mathrm{Bt}}}$ and $\overline{\mathrm{Rec}_{\mathrm{Nst}}}$ are the average of the recommendations collected after Δt time, respectively, and n is the number of neighbor nodes.

After calculation of $\overline{\mathrm{Rec}_{\mathrm{Bt}}}$ and $\overline{\mathrm{Rec}_{\mathrm{Nst}}}$, the relative deviation of the trust metrics of node k (monitored node) are represented as follows:

$$\mathrm{Dv}_{\mathrm{Bt}} = \frac{\overline{\Delta \mathrm{Rec}_{\mathrm{Bt}}(t)} - \Delta \mathrm{Bt}_k(t)}{\overline{\Delta \mathrm{Rec}_{\mathrm{Bt}}(t)}},$$
$$\mathrm{Dv}_{\mathrm{Nst}} = \frac{\Delta \mathrm{Nst}_k(t) - \overline{\Delta \mathrm{Rec}_{\mathrm{Nst}}(t)}}{\overline{\Delta \mathrm{Rec}_{\mathrm{Nst}}(t)}}, \tag{11}$$

where $\mathrm{Dv}_{\mathrm{Bt}}$ and $\mathrm{Dv}_{\mathrm{Nst}}$ are the deviations of trust metrics, respectively. $\Delta \mathrm{Bt}_k(t)$ is $\mathrm{Bt}_k(t-\Delta t) - \mathrm{Bt}_k(t)$ and $\Delta \mathrm{Nst}_k(t)$ is $\mathrm{Nst}_k(t-\Delta t) - \mathrm{Nst}_k(t)$. $\mathrm{Bt}_k(t)$ denotes the back-off time at time t and $\Delta \mathrm{Bt}_k(t)$ is the back-off time during Δt time (between node j and node k).

Now, we calculate the individual trust using the Bt and Nst parameters as follows:

$$T_{jk}^{\mathrm{Bt}}(t) = \begin{cases} 1 - \mathrm{Dv}_{\mathrm{Bt}}(t), & \text{if } \Delta \mathrm{Bt}_k(t) < \overline{\Delta \mathrm{Rec}_{\mathrm{Bt}}(t)}, \\ 1, & \text{else}, \end{cases} \tag{12}$$

$$T_{jk}^{\mathrm{Nst}}(t) = \begin{cases} 1 - \mathrm{Dv}_{\mathrm{Nst}}(t), & \text{if } \Delta \mathrm{Nst}_k(t) > \overline{\Delta \mathrm{Rec}_{\mathrm{Nst}}(t)}, \\ 1, & \text{else}. \end{cases} \tag{13}$$

From equations (12) and (13), it is observed that when $\Delta \mathrm{Bt}_k(t)$ is lesser than average, the node is less trustworthy, and when $\Delta \text{Nst}_k(t)$ is greater than average the node has less trustworthiness. The final trust at the MAC layer is calculated as follows:

$$T_{jk}^{\text{MAC}}(t) = \beta_1 \times T_{jk}^{\text{Bt}}(t) + \beta_2 \times T_{jk}^{\text{Nst}}(t), \tag{14}$$

where β_1 and β_2 belong to [0, 1] and the sum is 1 ($\beta_1 + \beta_2 = 1$). The value of β_1 and β_2 depends on the IDS system. The value of β depends on the IDS. These weight factors β_1 and β_2 describe the priority of back-off time and the number of successful message transmission to generate the trust value of a node at the MAC layer.

4.3. Estimation of Network Layer Trust. At the network layer, hop count hp is considered as the trust metric to calculate the deviation. The network layer of the protocol layer is mainly used for routing. Therefore, hop count is used as the route metric for the successful delivery of the message. According to the sinkhole attack at the network layer, a malicious node advertises bogus route information. It may advertise low hop count in the path for reliable data delivery. Therefore, hp is considered as the trust metric for trust estimation at the network layer. Here, the monitoring node j collects recommendations from its neighbor nodes after the time period Δt. These recommendations are the hp values generated by direct experience of the neighbor nodes with monitored node k. The average of the recommendations (hp) is calculated as follows:

$$\overline{\text{Rec}_{\text{hp}}} = \frac{1}{n}\sum_{i=1}^{n} \text{hp}_n, \tag{15}$$

where $\overline{\text{Rec}_{\text{hp}}}$ is the average of the recommendations collected after Δt time and n is the number of neighbor nodes.

After calculation of $\overline{\text{Rec}_{\text{hp}}}$, the relative deviation of the trust metric of node k (monitored node) is represented as follows:

$$\text{Dv}_{\text{hp}} = \frac{\overline{\Delta\text{Rec}_{\text{hp}}(t)} - \Delta\text{hp}_k(t)}{\overline{\Delta\text{Rec}_{\text{hp}}(t)}}, \tag{16}$$

where Dv_{hp} is the deviation of trust metric. $\Delta\text{hp}_k(t)$ is $\text{hp}_k(t-\Delta t) - \text{hp}_k(t)$. $\text{hp}_k(t)$ denotes the hop count at time t and $\Delta\text{hp}_k(t)$ is the hop count during Δt time (between node j and node k).

Now, we calculate the individual trust using the hp as follows:

$$T_{jk}^{\text{hp}}(t) = \begin{cases} 1 - \text{Dv}_{\text{hp}}(t), & \text{if } \Delta\text{hp}_k(t) < \overline{\Delta\text{Rec}_{\text{hp}}(t)}, \\ 1, & \text{else.} \end{cases} \tag{17}$$

From equation (17), it is observed that when $\Delta\text{hp}_k(t)$ is lesser than the average the node has less trustworthiness. Here, $T_{jk}^{\text{hp}}(t)$ is the trust $T_{jk}^{\text{NET}}(t)$ at the network layer.

5. Analysis of LB-IDS

In this section, we have analyzed the message complexity, memory overhead, energy consumption, and trust evaluation of LB-IDS.

5.1. Message Complexity. The message complexity of LB-IDS scheme depends on the individual trust calculation of a layer. Let there exists a clustered WSN, where c denotes the number of clusters existing, and the average number of SNs in a cluster is n. If the average number of neighbors for an SN is p, then $n \times p$ communication occurs to calculate the overall trust values of the SNs in a cluster in Δt time. Therefore, the message complexity to calculate the overall trust $T_{jk}(t)$ of all SNs in a cluster is $O(n \times p)$. For c clusters, the time complexity of the clustered WSN is $O(n \times p \times c)$.

Figure 7 shows the message overhead in a cluster network with 50 SNs. According to LB-IDS, if node j estimate the trust value of node k then it requires a recommendation message from those n neighbors those have a direct experience with node k. Then, the total number of messages N to compute the trust value of k is n. For 50 SNs, the total number of messages is $50 \times n_{\text{avg}}$, where n_{avg} is the number of average neighbors that provides the recommendation message. From Figure 7, it is observed that when the number of average neighbors increases, the number of messages in the network also increases.

5.2. Memory Overhead. From the above scenario, if a single cluster is considered, then $n \times p$ communication occurs to calculate the overall trust values in a cluster. If a recommendation message of length l_{M} bits is received from a neighbor node for trust calculation, then the whole cluster requires $(n \times p \times l_{\text{M}})$ memory overhead. Hence, the memory overhead to calculate the overall trust values of a clustered WSN is $(n \times p \times c \times l_{\text{M}})$.

5.3. Energy Consumption. From the above scenario, if a single cluster is considered, then $n \times p$ communication occurs to calculate the overall trust values of a cluster. Let a message of length l_{M} bits is transmitted from a neighbor node for trust calculation, and the energy consumed is η joules. For receiving the message, let energy consumed is ρ joules. Then, the whole cluster consumes $(n \times \rho + n \times p \times \eta)$ joules. Therefore, the energy consumption of the clustered WSN is $(n \times \rho + n \times p \times \eta) \times c$ joules during Δt time.

Figure 8 shows the energy consumption in a cluster network with 50 SNs. According to LB-IDS scheme, if a node j estimates the trust value of node k, then it requires a recommendation message from those n neighbors those have a direct experience with node k. The message size in this simulation is considered to be 4 bytes, and the energy consumption is taken as 3.12 μJ/bit [49]. Hence, for 4 bytes transmission, 99.84 μJ energy is consumed. For receiving a message of size 4 bytes, 74.88 μJ energy is consumed because the energy consumption to receive a bit is taken as 2.34 μJ [49]. From Figure 7, it is observed that when the number of average neighbors increases the energy consumption also increases in the network.

5.4. Trust Evaluation. In LB-IDS, we have considered the trust calculation of an SN using the direct experience and experience of the neighbor nodes with node k. Therefore, the

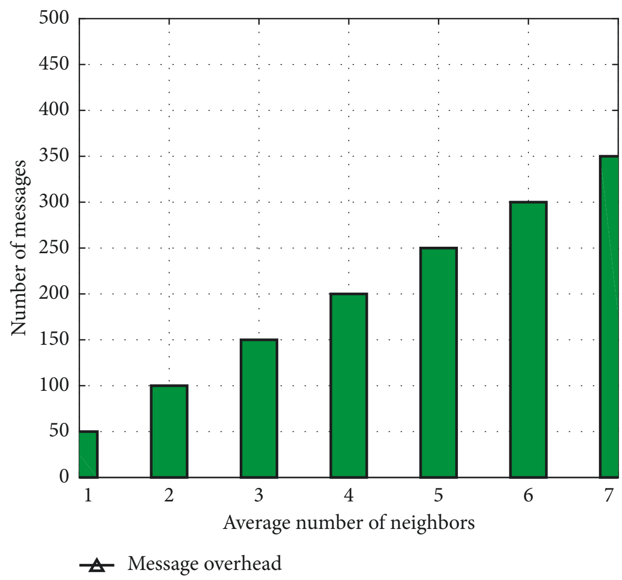

Figure 7: Memory overhead in a clustered WSN.

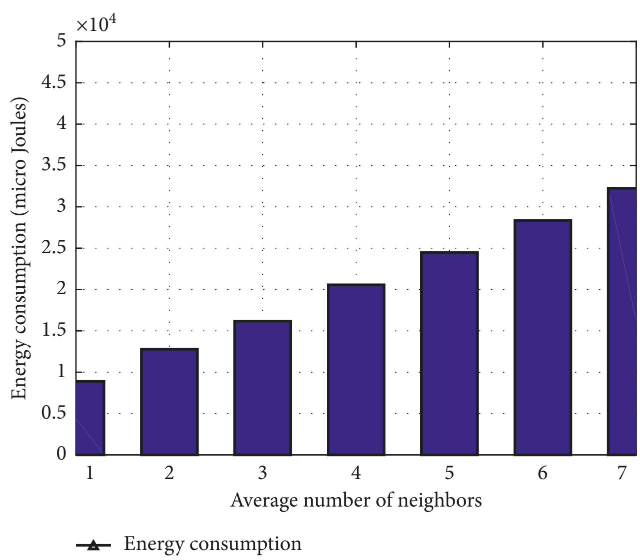

Figure 8: Energy consumption in a clustered WSN.

hybrid of indirect experience and direct experience gives better detection accuracy because in direct trust computation, the monitoring node uses only its experience with other nodes, which may be incorrect.

6. Results and Discussion

The performance of LB-IDS is evaluated by comparing the results of the three performance metrics such as detection accuracy, false-positive rate (FPR), and false-negative rate (FNR) with the results of Wang's scheme. Detection accuracy calculates the accuracy of IDS in detecting the malicious nodes. FPR and FNR calculate at what ratio the detection accuracy is true or false. The computer simulations are performed using MATLAB R2015a. The machine in which the simulation is performed has 6 Gb RAM, core i7 processor, and Windows 10 platform. The LB-IDS scheme is compared with the most recent Wang et al. [1] scheme, which is also based on protocol layer trust. The performance metrics for the simulation are defined as follows:

(1) Detection accuracy: the number of malicious SNs detected from the total number of malicious SNs present in the network.

(2) False-positive rate (FPR): the number of genuine SNs detected as malicious from the total number of genuine SNs.

(3) False-negative rate (FNR): the number of malicious SNs detected as genuine from the total number of malicious SNs.

6.1. Simulation Setup. The simulation is set in an area of size $100 \times 100\,m^2$. The area is considered as a cluster network with 1 CH and 50 sensor nodes. The nodes are randomly deployed using the coordinates (x, y), which are generated using randi(). The communication range of an SN is set to be 20 m. In this simulation, we have considered 4 types of attack such as (1) jamming attack, (2) back-off manipulation attack, (3) sinkhole attack, and (4) cross-layer attack. To evaluate the LB-IDS scheme, we have varied the attackers from 2–25% of the SNs. For example, if 10% nodes are added as malicious, then 5 SNs are malicious in the network. At the physical layer, an SN is created as malicious by transmitting 1–10 messages of size 4 bytes during Δt time. Similarly, in this layer, a node is created as genuine by transmitting 1–3 messages of size 4 bytes. The Nmr is generated using the randi(). The energy consumption for sending a bit is $3.12\,\mu$J/bit [49]. At the MAC layer, the malicious SN is created by setting the back-off time between 10 and 25 μs. Similarly, for a genuine node, the back-off time is set between 20 and 30 μs. The Bt is generated using the randi(). At the network layer, a node is created as malicious by setting the hp between 1 and 2 and for a genuine node, it is set between 1 and 5. The hp is generated using randi(). The values of α_1, α_2, β_1, and β_2 are set to 0.5. We have considered equal weightage to all the parameters used for trust calculation in LB-IDS. When the jamming attack is implemented at the physical layer, then the value of λ_1 is taken as 1 and rest of λ_2 and λ_3 are taken as 0. Similarly, for the back-off manipulation attack at the MAC layer, $\lambda_2 = 1$, and the rest of the λ values are 0. For the sinkhole attack at the MAC layer, $\lambda_3 = 1$, and the rest of the λ values are 0. At the time of cross-layer attack implementation, λ_2 and λ_3 values are given equal weights (0.5) and λ_1 is considered as 0. Table 2 shows the simulation setup.

6.2. Results. Figure 9 shows the calculation of trust value of a malicious node under different types of attacks. It is observed that when a malicious node uses jamming attack, the trust value is below 0.8. Similarly, when a malicious node uses back-off manipulation attack, cross-layer attack, and

Table 2: Simulation setup.

Parameters	Values
Area	$100 \times 100\,\text{m}^2$
Number of SNs	50
Number of malicious nodes	2–25% of SNs
Communication range	20 m
Energy for transmit [49]	3.12 μJ/bit
Message size	4 bytes
Nmr for genuine node	1–3
Nmr for malicious node	1–10
Bt for genuine node	20–30 μs
Bt for malicious node	10–25 μs
Nst for genuine node	1–3
Nst for malicious node	1–10
hp for genuine node	1–5
hp for malicious node	1–2
μ, α_1, α_2, β_1, β_2	1/2
Number of iterations	10

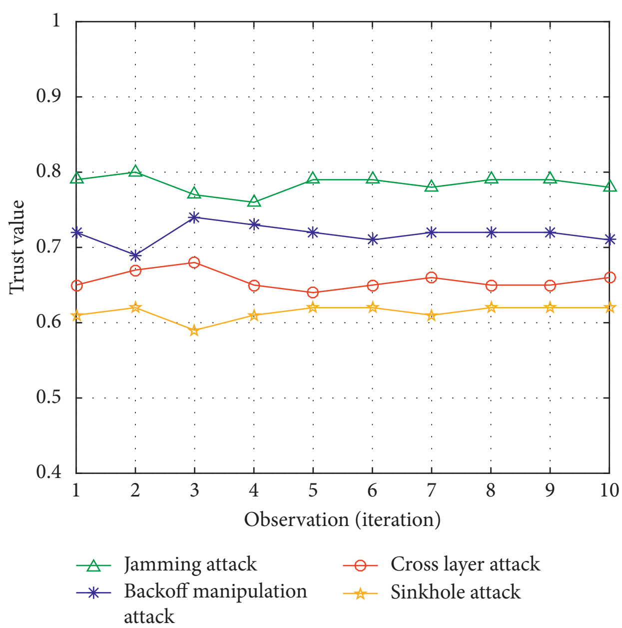

Figure 9: Trust values at different types of attacks.

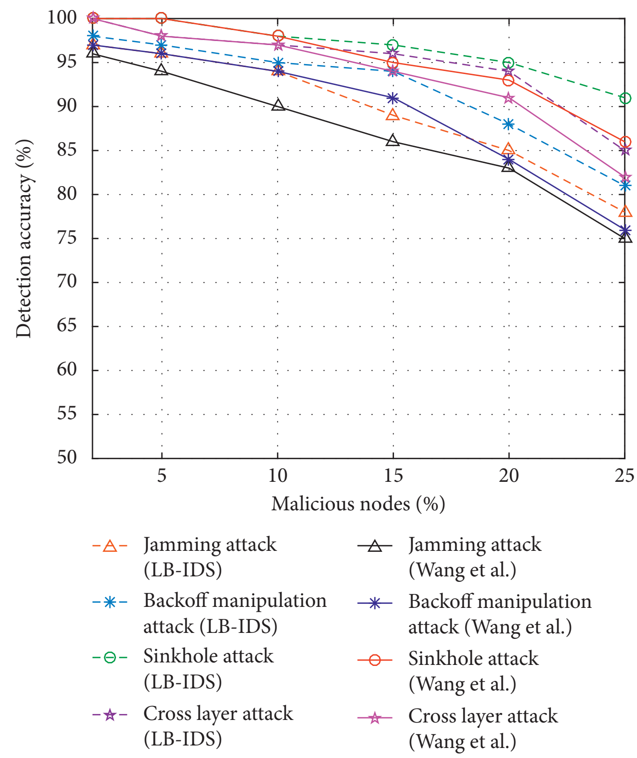

Figure 10: DA comparison between LB-IDS and Wang et al. scheme [1].

Table 3: Average of detection accuracy.

Attacks	Wang et al. [1]	LB-IDS
Jamming attack (%)	87.33	89.83
Back-off manipulation attack (%)	89.66	92.16
Cross-layer attack (%)	93.66	95
Sinkhole attack (%)	95.53	96.83

sinkhole attack, the trust values are below 0.74, 0.67, and 0.62, respectively. It is also observed that when the number of iterations or observations increases, the trust value gains stability. However, when the number of iteration is between 1 and 4, the trust value fluctuates due to less number of trust value data. From equation (2), we combined the previous experience with the current experience, and this leads to stability of the trust values. These trust threshold values are used to detect the malicious nodes in the network.

Figure 10 shows combined detection accuracy of Wang et al. [1] and LB-IDS scheme under different types of attacks. It is observed that the detection accuracy of LB-IDS is greater than Wang et al. [1] scheme under different attacks. From Table 3, it is observed that when the number of malicious nodes increases in the network, the average DA reduces. When jamming attack is implemented, the average detection accuracy of Wang et al. [1] and LB-IDS are 87.33% and 89.83%, respectively. When back-off manipulation attack is implemented, the average detection accuracy of Wang et al. [1] and LB-IDS are 89.66% and 92.16%, respectively. When cross-layer attack is implemented, the average detection accuracy of Wang et al. [1] and LB-IDS are 93.66% and 95%, respectively. When sinkhole attack is implemented, the average detection accuracy of Wang et al. [1] and LB-IDS are 95.53% and 96.83%, respectively.

Figure 11 shows the combined result comparison of LB-IDS with Wang et al. [1] scheme. It is observed that the FPR of LB-IDS is lower than that of Wang et al. [1] scheme under different attacks. From Table 4, it is observed that when the number of malicious nodes increases in the network, the average FPR increases. When jamming attack is implemented, the average FPR of Wang et al. [1] and LB-IDS are 18% and 15.66%, respectively. When back-off manipulation attack is implemented, the average FPR of Wang et al. [1] and LB-IDS are 15.16% and 13.16%, respectively. When cross-layer attack is implemented, the average FPR of Wang et al. [1] and LB-IDS are 10% and 8.66%, respectively. When

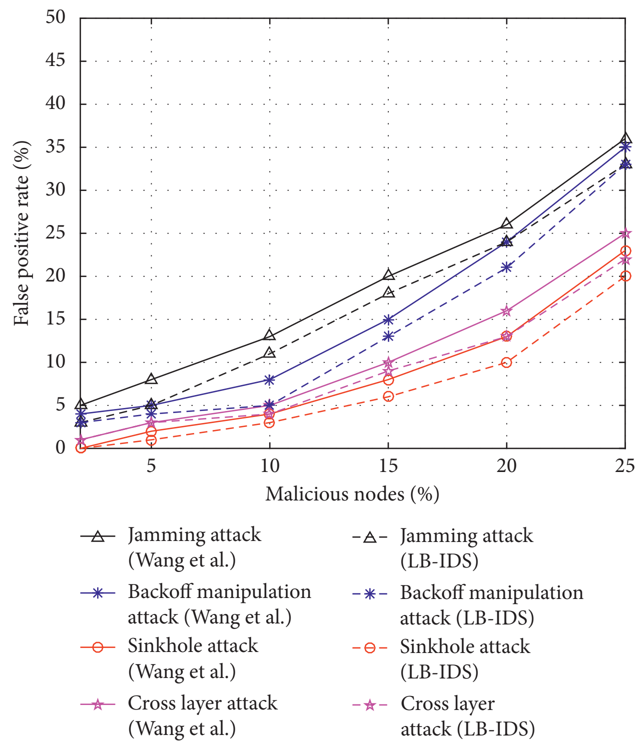

Figure 11: FPR comparison between LB-IDS and Wang et al. scheme [1].

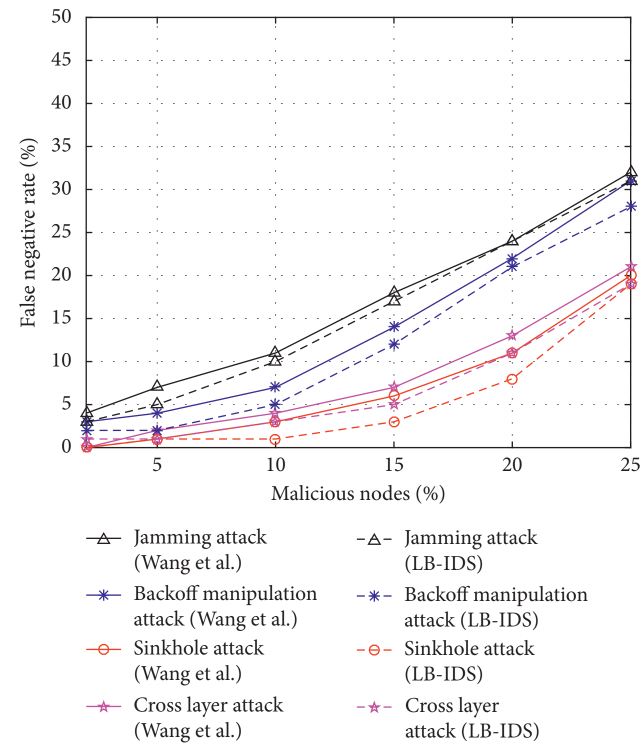

Figure 12: FNR comparison between LB-IDS and Wang et al. scheme [1].

Table 4: Average of false-positive rate.

Attacks	Wang et al. [1]	LB-IDS
Jamming attack (%)	18	15.66
Back-off manipulation attack (%)	15.16	13.16
Cross-layer attack (%)	10	8.66
Sinkhole attack (%)	8.33	6.66

Table 5: Average of false-negative rate.

Attacks	Wang et al. [1]	LB-IDS
Jamming attack (%)	16	15
Back-off manipulation attack (%)	13.50	11.66
Cross-layer attack (%)	7.8	5.33
Sinkhole attack (%)	6.8	6.66

sinkhole attack is implemented, the average FPR of Wang et al. [1] and LB-IDS are 8.33% and 6.66%, respectively.

Figure 12 shows the combined result comparison of LB-IDS with Wang et al. [1] scheme. It is observed that the FNR of LB-IDS is lower than that of Wang et al. [1] scheme under different attacks. From Table 5, it is observed that when the number of malicious nodes increases in the network, the average FNR increases. When jamming attack is implemented, the average FNR of Wang et al. [1] and LB-IDS are 16% and 15%, respectively. When back-off manipulation attack is implemented, the average FNR of Wang et al. [1] and LB-IDS are 13.50% and 11.66%, respectively. When cross-layer attack is implemented, the average FNR of Wang et al. [1] and LB-IDS are 6.8% and 6.66%, respectively. When sinkhole attack is implemented, the average FPR of Wang et al. [1] and LB-IDS are 8.33% and 6.66%, respectively.

7. Conclusion

The proposed LB-IDS secures the WSN by detecting the jamming attack, back-off manipulation attack, sinkhole attack, and cross-layer attack at the physical layer, MAC layer, and network layer, respectively. The threshold values of the trust at each layer are used for detecting the malicious nodes and genuine nodes in the network. From the results, it is observed that LB-IDS performs better than that of Wang et al. [1] scheme in terms of detection accuracy, false-positive rate, and false-negative rate. The analysis for LB-IDS is also performed in terms of message complexity, memory overhead, energy consumption, and trust evaluation. LB-IDS will be a better security solution for the clustered WSN. In future, we will implement and validate the proposed LB-IDS using wireless transceiver modules deployed in an outdoor environment.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Rajiv Gandhi National Fellowship (RGNF) Scheme funded by Ministry of Social

Justice and Empowerment and Ministry of Tribal Affairs, Govt. of India. We want to thank Berhampur University (Govt. of Odisha), India, for providing adequate infrastructure to conduct the experiments.

References

[1] J. Wang, S. Jiang, and A. Fapojuwo, "A protocol layer trust-based intrusion detection scheme for wireless sensor networks," *Sensors*, vol. 17, no. 6, p. 1227, 2017.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[3] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[4] R. R. Swain, P. M. Khilar, and S. K. Bhoi, "Heterogeneous fault diagnosis for wireless sensor networks," *Ad Hoc Networks*, vol. 69, pp. 15–37, 2018.

[5] M. Mohi, M. Ali, and P. Moradian Zadeh, "A bayesian game approach for preventing dos attacks in wireless sensor networks," in *Proceedings of WRI International Conference on Communications and Mobile Computing, 2009*, vol. 3, pp. 507–511, Yunnan, China, January 2009.

[6] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network mac protocols," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, pp. 367–380, 2009.

[7] X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan, "Sensor network configuration under physical attacks," in *Lecture Notes in Computer Science*, pp. 23–32, Springer, Berlin, Germany, 2005.

[8] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[9] W. Wenyuan Xu, K. Ke Ma, W. Trappe, and Y. Yanyong Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.

[10] S. Radosavac, A. A. Cárdenas, J. S. Baras, and G. V. Moustakides, "Detecting ieee 802.11 mac layer misbehavior in ad hoc networks: robust strategies against individual and colluding attackers," *Journal of Computer Security*, vol. 15, no. 1, pp. 103–128, 2007.

[11] R. Sokullu, D. Orhan, and I. Korkmaz, "On the ieee 802.15. 4 mac layer attacks: GTS attack," in *Proceedings of Second International Conference on Sensor Technologies and Applications, 2008*, pp. 673–678, Cap Esterel, France, August 2008.

[12] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile ad hoc networks," in *Proceedings of the 42nd Annual Southeast Regional Conference*, pp. 96-97, Huntsville, AL, USA, April 2004.

[13] I. Abdullah, M. Muntasir Rahman, and C. M. Roy, "Detecting sinkhole attacks in wireless sensor network using hop count," *International Journal of Computer Network and Information Security*, vol. 7, no. 3, pp. 50–56, 2015.

[14] N. James, E. Shi, D. Song, and P. Adrian, "The sybil attack in sensor networks: analysis & defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, pp. 259–268, Berkeley, CA, USA, April 2004.

[15] D. Nagireddygari and J. P. Thomas, "MAC-TCP cross-layer attack and its defense in cognitive radio networks," in *Proceedings of 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, pp. 71–78, Montreal, QC, Canada, September 2014.

[16] S. Radosavac, N. Benammar, and J. S. Baras, "Cross-layer attacks in wireless ad hoc networks," in *Proceedings of CISS*, Princeton, NJ, USA, 2004.

[17] J. Wang, A. O. Fapojuwo, C. Zhang, and H. Tan, "UML modeling of cross-layer attack in wireless sensor networks," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 104–115, 2016.

[18] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 266–282, 2014.

[19] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, "Trust-based secure clustering in wsn-based intelligent transportation systems," *Computer Networks*, vol. 146, pp. 151–158, 2018.

[20] S. Henningsen, S. Dietzel, and B. Scheuermann, "Challenges of misbehavior detection in industrial wireless networks," in *Ad Hoc Networks*, pp. 37–46, Springer, Berlin, Germany, 2018.

[21] P. Jokar and V. C. M. Leung, "Intrusion detection and prevention for zigbee-based home area networks in smart grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1800–1811, 2018.

[22] M. M. Alqhatani and M. G. M. Mostafa, "Trust modeling in wireless sensor networks: state of the art," *Journal of Information Security and Cybercrimes Research*, vol. 1, no. 1, 2018.

[23] Y. Zhang and W. Lee, "Intrusion detection in wireless ad-hoc networks," in *Proceedings of 6th Annual International Conference on Mobile Computing and Networking*, pp. 275–283, Boston, MA, USA, August 2000.

[24] X. Li, F. Zhou, and J. Du, "LDTS: a lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 6, pp. 924–935, 2013.

[25] N. Shao, Z. Zhou, and Z. Sun, "A lightweight and dependable trust model for clustered wireless sensor networks," in *Lecture Notes in Computer Science*, pp. 157–168, Springer, Berlin, Germany, 2016.

[26] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert systems with Applications*, vol. 29, no. 4, pp. 713–722, 2005.

[27] M. Moshtaghi, T. C. Havens, J. C. Bezdek et al., "Clustering ellipses for anomaly detection," *Pattern Recognition*, vol. 44, no. 1, pp. 55–69, 2011.

[28] E. P. K. Gilbert, B. Kaliaperumal, E. B. Rajsingh, and M. Lydia, "Trust based data prediction, aggregation and reconstruction using compressed sensing for clustered wireless sensor networks," *Computers & Electrical Engineering*, vol. 72, pp. 894–909, 2018.

[29] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data," *IEEE Access*, vol. 6, pp. 7234–7243, 2018.

[30] M. M. Ozcelik, E. Irmak, and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," in *Proceedings of 2017 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, Marrakech, Morocco, May 2017.

[31] T. Palpanas, D. Papadopoulos, V. Kalogeraki, and D. Gunopulos, "Distributed deviation detection in sensor networks," *ACM SIGMOD Record*, vol. 32, no. 4, pp. 77–82, 2003.

[32] R. R. Sahoo, S. Ray, S. Sarkar, and S. Kumar Bhoi, "Guard against trust management vulnerabilities in wireless sensor network," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 7229–7251, 2018.

[33] R. R. Sahoo, A. R. Sardar, M. Singh, S. Ray, and S. K. Sarkar, "A bio inspired and trust based approach for clustering in WSN," *Natural Computing*, vol. 15, no. 3, pp. 423–434, 2015.

[34] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345–1360, 2011.

[35] R. Wu, X. Deng, R. Lu, and X. Shen, "Trust-based anomaly detection in wireless sensor networks," in *Proceedings of 2012 1st IEEE International Conference on Communications in China (ICCC)*, pp. 203–207, Beijing, China, August 2012.

[36] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 3, p. 37, 2008.

[37] W. Luo, W. Ma, and Q. Gao, "A dynamic trust management system for wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 7, pp. 613–621, 2015.

[38] I. M. Atakli, H. Hu, Y. Chen, W. S. Ku, and S. Zhou, "Malicious node detection in wireless sensor networks using weighted trust evaluation," in *Proceedings of the 2008 Spring Simulation Multiconference*, pp. 836–843, Ottawa, Canada, April 2008.

[39] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: design considerations and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 2, pp. 107–130, 2013.

[40] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, "An efficient distributed trust model for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1228–1237, 2015.

[41] R. A. Shaikh, H. Jameel, B. J. D'Auriol, H. Heejo Lee, S. Sungyoung Lee, and Y.-J. Young-Jae Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698–1712, 2009.

[42] Z. Yao, D. Kim, and Y. Doh, "Plus: parameterized and localized trust management scheme for sensor networks security," in *Proceedings of 2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, pp. 437–446, Chengdu, China, October 2006.

[43] F. Ishmanov, S. Kim, and S. Nam, "A robust trust establishment scheme for wireless sensor networks," *Sensors*, vol. 15, no. 3, pp. 7040–7061, 2015.

[44] F. Bao, R. Chen, M.J. Chang, and J.-H. Cho, "Trust-based intrusion detection in wireless sensor networks," in *Proceedings of 2011 IEEE International Conference on Communications (ICC)*, pp. 1–6, Kyoto, Japan, June 2011.

[45] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[46] T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method for clustered wireless sensor networks based on cloud model," *Wireless Networks*, vol. 24, no. 3, pp. 777–797, 2016.

[47] G. Rajeshkumar and K. R. Valluvan, "An energy aware trust based intrusion detection system with adaptive acknowledgement for wireless sensor network," *Wireless Personal Communications*, vol. 94, no. 4, pp. 1993–2007, 2016.

[48] U. Ghugar, J. Pradhan, S. K. Bhoi, R. R. Sahoo, and S. K. Panda, "PL-IDS: physical layer trust based intrusion detection system for wireless sensor networks," *International Journal of Information Technology*, vol. 10, no. 4, pp. 489–494, 2018.

[49] M. G. C. Torres, *Energy consumption in wireless sensor networks using GSP*, Ph.D. thesis, University of Pittsburgh, Pittsburgh, PA, USA, 2006.