# Secure authentication and data aggregation scheme for routing packets in wireless sensor network

**Rudramurthy Veeregowdanadoddi Chandraiah[1], Aparna Ramalingappa[2]**
[1]Department of Computer Science and Engineering, Global Academy of Technology, Karnataka, India
[2]Department of Information Science and Engineering, Siddaganga Institute of Technology, Karnataka, India

**Article Info**

***Article history:***

Received Jul 27, 2022
Revised Sep 14, 2022
Accepted Oct 1, 2022

***Keywords:***

Consensus
Data aggregation
Dual layer integrated security
Feedback credibility
Reputation
Routing
Wireless sensor networks

## ABSTRACT

Wireless sensor networks (WSNs) comprise a huge number of sensors that sense real-time data; in general, WSNs are designed for monitoring in various application mainly internet of things based (IoT) application. Moreover, these sensors possess a certain amount of energy i.e., they are battery based; thus, the network model must be efficient. Furthermore, data aggregation is a mechanism that minimizes the energy; however, in addition, these aggregated data and networks can be subject to different types of attacks due to the vulnerable characteristics of the network. Hence it is important to provide end-to-end security in the data aggregation mechanism in this we design and develop dual layer integrated (DLI)-security architecture for secure data aggregation; DLI-security architecture is an integration of two distinctive layers. The first layer of architecture deals with developing an authentication for reputation-based communication; the second layer of architecture focuses on securing the aggregated data through a consensus-based approach. The experiment outcome shows that DLI identifies the correct data packets and discards the unsecured data packets in energy efficient way with minimal computation overhead and higher throughput in comparison with the existing model.

***Corresponding Author:***

Rudramurthy Veeregowdanadoddi Chandraiah
Department of Computer Science and Engineering, Global Academy of Technology
Bengaluru, Karnataka, India
Email: rudramurthy.vc@gmail.com

## 1. INTRODUCTION

Wireless sensor networks (WSNs) are often comprised of a large amount of low-cost, low-power detecting devices having constrained storage, computing, and transmission capabilities [1], [2]. The WSNs could provide a low-cost solution to a wide range of challenges in the army and for commercial uses, such as military surveillance, target detection, health, and environment care surveillance, wildfire monitoring, and traffic management. The typical data transmission architecture consists of sensor nodes, cluster heads, and base stations. Sensor nodes contain minimal hardware and significant resource limitations because of the reduced implementation cost requirements of the WSNs [3]. As a result, providing an appropriate resolution to the information collection issue is a difficult challenge. Between those constraints, the most restrictive component in building WSN protocols is battery power. As a result, numerous strategies have been presented to lower the energy utilization of WSNs, including wireless scheduling, packet transmission removal, topology management, and, most critically, data aggregation [4].

The data aggregation technique reduces the consumption of energy consumption and eliminates redundant information. The sensing nodes are placed as a tree-like structure during the stage of aggregation of data, with the access point at the root. The information coming through the leaf nodes is consolidated by the transitional sensing nodes, which subsequently send the consolidated output information to the root access point. This technique causes complications in certain systems, including healthcare monitoring systems. Sensing nodes are commonly placed in hostile environments [5], [6] with limited bandwidth and unpredictable communication channels [7], [8]. This may enable hostile information modifications and data fabrication, resulting in a breach of the user's privacy. For example, an attacker may forge a duplicated alert reading and distribute it around the system to degrade the system's performance. Moreover, privacy must be protected in healthcare monitoring observation devices because the information obtained through the device is only important to the patient being monitored. For example, motion sensors can detect whether the patient is moving, eating, or resting. The disclosure of these kinds of health-related information has consequences because it violates the patient's privacy. So, in a restricted resource environment, an effective method of collecting varied inputs and securely storing patient information is necessary. Furthermore, WSNs are vulnerable to many potential attacks on their location, communication channels, and lack of physical security [9]–[11]. Various sorts of vulnerabilities really can affect the system and network during the aggregation of data stage, some of them are listed below [12].

Service denial: this technique is also known as a routing attack since it emits wireless signals to disrupt the frequency used by WSN. If the strength of the opponent's wireless signals increases, much of the network will be disrupted. Even during the aggregation process, this technique can force the aggregating nodes to prevent data from flowing to higher levels. This assault is also known as a node compromise attack. Supervision attack: in this attack, the attacker removes all the information contained in the node. If the nodes are taken by this approach, the node's entire secured information will be erased throughout the aggregation of data stage. Sybil attack: in this attack, the attacker can generate several recognitions within the system throughout this form of attack. The data-aggregation is altered using several methods because of this attack, including: i) The attacker will induce multiple recognitions to generate additional votes for the aggregation voting scenarios and chooses a malicious node for the data aggregation. If the attacker is permitted to generate many inputs with non-identical values, then the resulting aggregation can be illegitimate; ii) The attacker can launch this technique and generate n or more recognitions. Due to this, the access point is then forced to receive the aggregation result. Selective forwarding attack: in this attack, the denial of any hacked node to send the acquired information because the attacker has authority over that hacked node and can tell the nodes not to transmit or reject the information. These forms of attacks have an impact on the aggregation outcomes. Replay attack: in this attack, the attacker will monitor the network traffic and without being conscious of it, the attacker could replay the network traffic in a subsequent interval to mislead the aggregator, affecting the aggregator's outcome. Secret attack: this attack involves the injection of incorrect data into the network without disclosing its presence. Because the inserted incorrect information is added to the original aggregate process, hence, the aggregation results will change.

Rapid development in the WSN environment has developed a dynamic application in almost every area of application including the hazardous environment. Moreover, WSN generates a huge amount of data which causes data redundancy; the issue of data redundancy is solved through data aggregation. In data aggregation, there are two major issues. The first issue relates the efficient data aggregation, and the second issue is related to secure data aggregation; further motivated by the application-based environment we design and develop dual-layer architecture. Dual layer architecture follows the authentication, efficient and secure data aggregation. Further, the research contribution of the research article can be highlighted below points: i) the work designed and develop a dual layer-based architecture to provide reputation-based communication and secure data aggregation; ii) the first layer of the security architecture focuses on establishing a reputation for communication among the nodes whereas the second layer deals with the efficiency and security in data aggregation through a consensus-based approach; and iii) the proposed model is evaluated considering the parameter i.e., energy consumption; further comparative analysis is carried out considering the true packet identification and false packet identification. The false packet is the insecure one.

The research paper has been organized in the following way; the section 1 starts with the background of the sensor network, its application, the problem associated with the WSN, and the security concern is highlighted. The section 2 focuses on the different related work along with the shortcomings of the model. The section 3 deals with the proposed approach along with the mathematical formulation whereas the proposed model is evaluated in section 4 along with the comparative analysis.

## 2. RELATED WORK

In [13], the multiple description coding (MDC) route is found by using terrain effect to save energy consumption and cost. In [14], relaying systems and MDC have been used in a simulated scenario. In [15], data aggregation visualizes both collision avoidance and obstacle detection. In [16], they have investigated the problem of privacy-protecting data aggregation in the context of a cyber-physical approach. Further, Chen *et al.* [17] have modeled a blockchain-based sharing cloud architecture with fog nodes that are referred to as software-defined networking. Nonetheless, due to the typical block header concept and block production techniques, these techniques will not meet the security requirements based on data aggregation. Yan *et al.* [18] have described a safe and energy-efficient aggregation of data technique that executes offloading for fog-aided internet of things networks. The construction of this three-layer secured, fog-aided architecture is done specifically to react to any security threat and begin the aggregation procedure like encrypted text. Meanwhile, a momentum descent-based energy efficiency offloading technique is modeled to reduce the overall energy consumption of the methods of execution. With a higher convergence speed, this can achieve the minimum value. Finally, the security and computation-based analysis revealed that the modeled data aggregation approach is an effective data processing method that achieves a significant breakthrough in the energy consumption method. In this method, a group-dependent key generation mechanism was first defined.

Meters were grouped into groups, and the meters in that group developed the keys for the encryption of the data, reducing the issue of the meter failing. If there is a faulty meter in any of the categories, then the other categories will be unaffected. Moreover, by allowing meters to update their keys, different processes such as dynamic join, leave, and replacement of meter methods are defined. Furthermore, in addition to the method, a few techniques that were able to give secure data aggregation are reviewed in [18]–[20]. In [18], the created method can check on its own, and reliability is proven, although it is restricted owing to its complexity and restricted range of adoption. Similarly, Zhang *et al.* [19] used a compressive sensing-based data aggregation security strategy, where compressive sensing was prioritized over security. Other work, such as [20], is developed for internet of things (IoT)-based applications to solve the complexities of all the above paradigms; while the technique appears to be adaptive, it is limited and lacks dynamic adoption. Further, studies [21]–[24] used the blockchain approach to secure the network whereas [25] used the user privacy approach to preserve privacy in data aggregation. Even if all the above-mentioned works can achieve good data aggregation for future-generation WSNs [26], [27], there are two unsolved issues still: how can the protected data aggregation be executed? also under this scenario, how can energy-saving data aggregation be performed?

## 3. PROPOSED METHOD

The necessity of data aggregation along with the security model has led several researchers to work on the secure data aggregation problem [28], [29]. Hence, in this research work, we design and develop a dual-layer architecture for secure data aggregation as shown in Figure 1. First layer deals with the authentication model and second layer architecture deals with the consensus-based data aggregation. Moreover, the first layer mainly deals with developing reputation-based communication whereas the second layer provides absolute security in data aggregation.

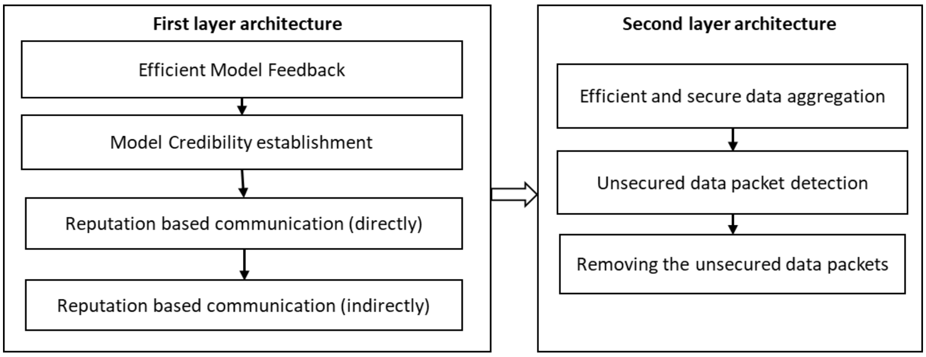
First layer architecture
Efficient Model Feedback
Model Credibility establishment
Reputation based communication (directly)
Reputation based communication (indirectly)
Second layer architecture
Efficient and secure data aggregation
Unsecured data packet detection
Removing the unsecured data packets

Figure 1. Dual layer-integrated secure architecture

### 3.1. Reputation-based secure communication

In the first layer of architecture, this research aims to develop reputation-based communication which is used for authentication of node in WSNs. In order to achieve reputation-based communication, a different sublayer of the architecture is introduced. Moreover, this layer assures reputation. The sublayer is composed of feedback model, credibility model, direct and indirect communication model. Then, after computing all these sublayer reputation metrics, the final reputation metric is obtained for authenticating nodes in WSNs.

#### 3.1.1. Feedback model

The WSNs is a cluster-based model, at first, we compute the reputation-based communication [30] where the sensors comprise the trust level information of transmission; let us consider $\zeta_p^v(y,z)$ which is a parameter for reputation-based communication between sensor devices $y$ and $z$ with $p$ interaction along with $u$ session period. Further, the updation in reputation-based communication can be formulated through (1).

$$\zeta_p^v(y,z) = \alpha * \zeta_{rec}(y,z) + (1-\alpha) * \zeta_{p-1}^v(y,z). \tag{1}$$

where $p$ defines the current instance set as 0 and $v$ defines the $v^{th}$ time instance. In (1), $\alpha$ is an optimization parameter with collected variance [31]. More details of how the $\alpha$ is computed can be obtained from [31]. Furthermore, we consider the feedback-aware secure approach where feedback is taken to understand the quality of experience (QoE), and this can be formulated as (2).

$$\zeta_{rec} = \begin{cases} 0, \ if\ interaction\ completely\ untrustable, \\ 1, \ if\ interaction\ is\ completely\ trustable, \\ \qquad \in (0,1), \quad otherwise. \end{cases} \tag{2}$$

Further, we develop the feedback which can be represented through (3); where $q$ represents a common sensor device, $I(y,z)$ depicts a common sensor device with whom sensor devices $y$ and $z$ have interacted:

$$W_p^v(y,z) = \sqrt{\frac{\sum_{q\in I}\left(\zeta_p^v(y,q)-\zeta_p^v(z,q)\right)^2}{|I(y,z)|}} \tag{3}$$

where $I(y,z)$ defines the common node $q$ with whom $y$ and $z$ have an association. Further, for establishing an association between sensor device $y$and $z$ (i.e., $\left(S_p^v(y,z)\right)$), sensor device $y$ first estimates $W_p^v(y,z)$, and updates the association using (4).

$$S_p^v(y,z) = \begin{cases} S_{p-1}^v(y,z) + \frac{1-S_{p-1}^v(y,z)}{Y}, \ if W_p^v(y,z) < I, \\ \quad S_{p-1}^v(y,z) - \frac{1-S_{p-1}^v(y,z)}{Z}, \ else, \end{cases} \tag{4}$$

where $Y$ depicts the reward parameter and $Z$ depicts the penalty parameter, and both parameters can be modified in a dynamic nature based on system security requirements.

#### 3.1.2. Credibility model

Let $G_p^v(y,z)$ defines the feedback credibility of sensor device $z$ from sensor device $y's$ point of view can be estimated using (5).

$$G_p^v(y,z) = \begin{cases} 1 - \frac{\log\left(\zeta_p^v(y,z)\right)}{\log\theta}, \ if\ S_p^v(y,z) > \theta, \\ \qquad 0, \ else \end{cases} \tag{5}$$

where $\log\theta$ depicts the least tolerable parameter of similarities. In this work logarithm computation is considered because the reputation value should gradually increase/decrease.

#### 3.1.3. Reputation-based communication through direct way

Let $M_p^v(y,z)$ represent the direct trustable value that sensor device $y$ has upon sensor device $z$ with at least $p$ interaction in $v^{th}$ session instance. Using a trustable metric, the direct trust is computed using (6).

$$M_p^v(y,z\ ) = \zeta_p^v(y,z). \tag{6}$$

Thus, using (6) if the sensor device $z$ gives better transmission performance, then sensor device $y$ will give an ideal trustable parameter. This aid sensor device $z$ to attain better trustable parameters from $y's$ sensor device point of view.

### 3.1.4. Reputation-based communication through an indirect way

The sensor device aggregates the feedback of other sensor devices for computing indirect using (7).

$$H_p^v(y,z) = \begin{cases} \frac{\sum_{q\in A-\{y\}} G_p^v(y,z)*M_p^v(y,z\ )}{\sum_{q\in A-\{y\}} G_p^v(y,z)}, \ if\ |A-\{y\}|>0,\ if\ |A-\{y\}|=0 \\ 0 \end{cases} \tag{7}$$

where $A = T(z)$ depicts the sensor device set that interacted with sensor device $z$. Let $D_p^v(y,z)$ describes the present trustable parameter that sensor device $y$ has upon sensor device $z$.

$$D_p^v(y,z) = \xi * M_p^v(y,z\ ) + (1-\xi) * H_p^v(y,z) \tag{8}$$

where $\xi$ depicts the weight of the trustable parameter which is measured through the ratio of total interaction with total interaction plus mean interaction like [28]. Let $M_p^v(y,z\ )$ describes the historical trust parameter that sensor device $x$ has upon sensor device $y$.

$$M_p^v(y,z\ ) = \frac{\psi * M_p^v(y,z\ ) + D_{p-1}^v(y,z)}{2}, \tag{9}$$

where $\psi (0 \leq \psi \leq 1)$ is the reward parameter and$M_p^0(y,z) = 0$. By using the historical trust parameter, current malicious sensor devices interacting with specific sensor devices cannot quickly behave as ideal by overlooking previous behavior. Let $G_p^v(y,z)$ describes the future trustable parameter of sensor device $z$ from sensor device $y's$ point of view can be established using (10).

$$G_p^v(y,z) = \begin{cases} 0, if\ neither\ M\ or\ D\ is\ available \\ \vartheta D_p^v(y,z\ ) + (1-\vartheta) M_p^v(y,z\ )\ if\ eitherM\ or\ D\ is\ available \end{cases} \tag{10}$$

In our work $\vartheta$ is initially set to zero and it can be adjusted dynamically using deviation factor $\varrho$. Nonetheless, the value of $\varrho$ is not kept very small; because the attacker may come out of a bad state to good. Next, the work introduces a new penalty function for idle sensor node that has not yet participated for a longer period. Here the trust value is reduced as time passes for the sensor node that does not communicate for a longer period. In this work, the reputation function of (1) is optimized as both direct and indirect communication metrics rely on it.

$$\hat{\zeta}_p^v(y,z) = \zeta_p^v(y,z) e^{-\beta \Delta v}. \tag{11}$$

The parameter $\beta$ defines how fast the reputation value reaches zero and becomes an untrustable node. The parameter $\Delta v$ defines the session window gap between the current and last interaction which is computed using (12).

$$\Delta v = v_{cur} - v_{prev} \tag{12}$$

The usage of the penalty function improves the reliability of wireless sensor networks. Here we cumulate the biased and fluctuating trust parameter for computing fluctuation using (13).

$$E_p^v(y,z) = \begin{cases} E_{p-1}^v(y,z) + \frac{D_p^v(y,z\ ) - M_p^v(y,z\ )}{\rho},\ if D_p^v(y,z\ ) - M_p^v(y,z\ ) > \varsigma \\ E_{p-1}^v(y,z) + M_p^v(y,z\ ) - D_p^v(y,z\ ),\ if D_p^v(y,z\ ) - M_p^v(y,z\ ) > -\varsigma \\ E_{p-1}^v(y,z),\ otherwise, \end{cases} \tag{13}$$

where $\varsigma$ describes the tolerance parameter of credibility error in estimating the trustable parameter and $\rho (\rho > 1)$ describes the penalty parameter for fluctuation in the trustable parameter; Therefore, biased, and fluctuating trust of a sensor device using (13) can be established using (14).

$$\bar{\bar{E}}_p^v(y,z) = \begin{cases} 0,\ if\ E_p^v(y,z) > E \\ \cos\left(\frac{\pi}{2} * \frac{E_p^v(y,z)}{\max E_p^v(y,z)}\right),\ otherwise, \end{cases} \tag{14}$$

where $E$ defines the total bias parameter of WSNs. The final security metric $G_p^v(y,z)$ is established using the future trust parameter and fluctuating trust parameter and is evaluated using (15).

$$G_p^v(y,z) = G_p^v(y,z) * \bar{\bar{E}}_p^v(y,z). \tag{15}$$

From (15), it can be stated that sensor devices with higher future trust parameter outcomes but with low fluctuation trust parameter outcomes will ultimately result in having low overall trustable outcomes. In another way, a sensor device that intentionally changes the state between fluctuating trust parameters will have a lower trustable parameter because of its low fluctuation trust parameter. Thus, for balancing load $U^v(y,z)$ among cluster head this work first estimates the traffic (i.e., energy overhead) at the sensor device using (16).

$$U^v(y,z) = \mathcal{U}^v(y,z) + \sum_{q\in A-\{y\}} G_p^v(y,q) * \mathcal{U}^v(q,z) \tag{16}$$

where $\mathcal{U}^v(y,z)$ defines the number of interactions the sensor node $y$ had with sensor node $z$. Furthermore, the selected CH for transmitting packet is established using (17).

$$\min \sum_{q\in A-\{y\}} U^v(y,q) \tag{17}$$

Further, initially, some newly joined sensor devices may not have any trustable value. For such cases, this work chooses a sensor device probabilistically using (18):

$$Q^v(y,z) = \begin{cases} \frac{G_p^v(y,z)}{\sum_{q\in w} G_p^v(y,q)},\ if\ \sum_{q\in w} G_p^v(y,q) \neq 0, \\ arbitrarily\ choose\ any\ sensor\ device,\ else. \end{cases} \tag{18}$$

For selecting a sensor device from $w$, this work utilizes (18) with a high trustable parameter, the sensor device with a high trustable parameter is having a better probability of getting chosen. However, when the trustable parameter is zero the sensor device is chosen randomly.

### 3.2. Integrity aware data aggregation

Since once the reputation-based communication is established then data aggregation is carried out; moreover, to secure data aggregation, we develop a consensus-based approach [32] which tends to discard the unsecured packets; also, we tend to provide an efficient way where energy is taken into consideration. Reputation-based communication is established first, then the data aggregation is carried out. we develop a consensus-based approach [32] for secure data aggregation. This approach tends to discard the unsecured packets; also, we tend to provide an efficient way where energy is taken into consideration.

#### 3.2.1. Consensus-based efficient and secure data aggregation

In achieving the best security for the data, assume the aggregated data as $z_k$and additional noise as $\delta_k$with a gaussian-distribution; we then define the final data, which would be the additional noise as well as the detected data from WSN, as (19).

$$\tilde{z}_k = x_k + \delta_k \tag{19}$$

The added noise in the preceding formula is almost equivalent to the $\delta_j \sim O(0,\sigma^2)$; additionally, using the approximation, the (19) can be stated as (20).

$$\hat{A}^m = \sum_{k=1}^{P'} y_k^m \tilde{z}_k^m\ , \tag{20}$$

where $P'$ denotes the legitimate information between all information; extra noise is included using a randomized generating mechanism. Furthermore, the chosen randomized function is supplied as $O(.)$ to the original detected information $z_k$ and can be expressed as $\tilde{y}_k = O(z_k)$=$z_k + \delta_k$. When we build the manipulated, which is a combination of original detected information and new information, recognizing the original information becomes extremely difficult. Furthermore, an essential issue was discovered, namely the compromise among security and precision. To avoid this, we establish the incentive variable represented as $\zeta$. The incentive variable is calculated using $\zeta = [\bar{A} - A']$, where $\bar{A}$ signifies the appropriate mean taking $\hat{z}$ into account. The nominal value of variable $\zeta$ has superior data aggregation accuracy, according to the variable description and assessment. Furthermore, we may calculate the actual sensed information using the specified number of participants, session time $z_k^m$, and weights $y_k^m$ using the (21).

$$A^m = \sum_{k=1}^{P} y_k^m z_k^m \tag{21}$$

### 3.2.2. Detection of the unsecured packet in the network

Every data aggregation can be trusted, but it can only be verified if it meets the data aggregation quality requirements; thus, we provide a method for identifying dishonest nodes. This could be accomplished by following the steps outlined under. Let us define $J_0$ as any data-aggregation variable for efficiency, while $J_1$ indicates non-efficiency, and therefore we can construct a formula for the packet misidentified, i.e., the number of nodes that really are honest and are therefore not evaluated as such $R_h = R(J_1|J_0))$. Furthermore, the misclassification rate can be represented as $R_m$, where the dishonest packet is treated as the honest one; this can be represented as $R_m = R(J_0|J_1)$. As a result, we develop the static test and express it as (22).

$$N = \| z_k^m - \hat{z}_k^m \|^2 \tag{22}$$

The equation offers the variation between the two specified terms in (2). Assume the information $z_k = (z_k^1, z_k^2, \dots\dots, z_k^p)$. Furthermore, the testing for correctly categorized and incorrectly categorized packets is designed as $N \lessgtr_{J_1}^{J_0} (\vartheta)$. Therefore, if the information is true, the participants are modified; otherwise, it is rejected, as shown by (23).

$$\begin{gathered} z_k^m \leftarrow z_k^m \\ \text{Else} \\ z_k^m \leftarrow z_k^{m-1} \end{gathered} \tag{23}$$

Assume an energy parameter, where the energy limitation is of complete packets which are represented by $\mathbb{I}_1$, and the energy limitation of dishonest packets is represented by $\mathbb{I}_0$, where $\mathbb{I}_1 > \mathbb{I}_0 > 0$; finally, let's assume an attack probability variable, which can also be denoted by $p$ and likely threat is denoted by $T(\vartheta, r)$, so that any threat risk is calculated using (24).

$$T(\vartheta, r) = (\mathbb{I}_1(1 - R_h(\vartheta)) - ER_h(\vartheta))(1 - \sum_{k=1}^{P_o} r_k) + (\mathbb{I}_0(1 - R_m(\vartheta)) - ER_h(\vartheta)) \sum_{k=1}^{P_o} r_k \tag{24}$$

When the cluster function is represented as $vh_e(\vartheta, R)$, it could be shown that $vh_e(\vartheta, R) = T(\vartheta, r)$. Moreover, dual layer integration (DLI)-security mechanism is an integration of the first layer and second layer i.e., reputation and consensus respectively; these two layers contribute to DLI-security architecture. Furthermore, this mechanism is evaluated in the next section.

## 4. PERFORMANCE EVALUATION

In this section of the research, we evaluate the proposed model; moreover, the proposed model is evaluated by designing the specific network parameter described in [31]. Furthermore, evaluation is carried out on the windows 10 platform using the sensoria simulator; moreover, system architecture follows the 8 GB of Cuda-enabled Nvidia RAM and 1 TB of the hard disk. Furthermore, a sensoria simulator [33] is used for the simulation. Furthermore, various malicious nodes are generated to establish the efficiency of the model and security analysis, and the model performance is evaluated in terms of energy usage and network failed nodes. In addition, a comparison with the existing model [31], [32] is made in terms of malicious packet identification and throughput.

### 4.1. Network lifetime and communication overhead

Since the simulation is conducted by varying node size and fixing the attack rate to 20% the lifetime performance is studied using the proposed and existing secure routing model. The experiment outcome shows the proposed dual-layer security model achieves much better lifetime performance than the existing secure routing method. The lifetime performance enchantment of 52.9% is achieved using the proposed dual-layer security model over the existing secure routing method as shown in Figure 2. The simulation is conducted by varying node size and fixing the attack rate to 20% the communication overhead performance is studied using the proposed and existing secure routing model. The experiment outcome shows the proposed dual-layer security model achieves much better communication overhead performance than the existing secure routing method. The lifetime performance enchantment of 65.08% is achieved using the dual-layer security model over the existing secure routing method shown in Figure 3.

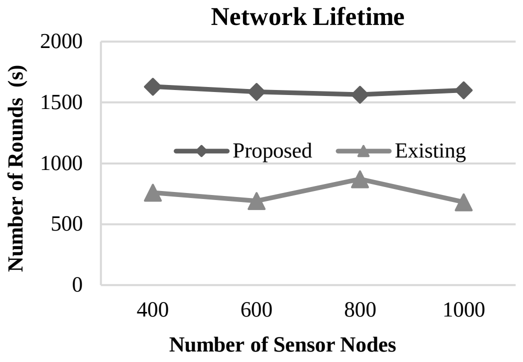

Figure 2. Lifetime study

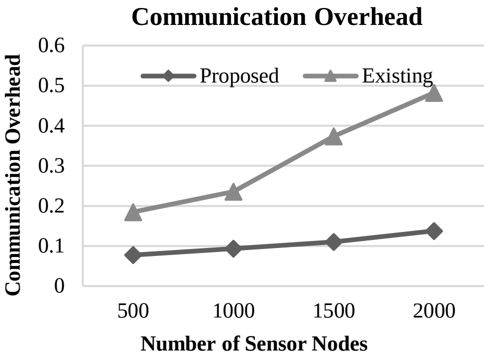

Figure 3. Communication overhead

### 4.2. True and false packet identification

The parameter identifying malicious devices expresses the data-aggregation mechanism's security issue; the bigger the number of packets identified, the more efficient the method is. Figure 4 depicts a comparative graph among the current and suggested models, with the x-axis indicating the number of sensor nodes triggered and the y-axis representing malicious packets. Moreover, in the scenario of 10% malicious devices, the existing system identifies 72 packets, but the suggested model identifies 84 packets. The current model identifies 63 packets in the instance of 20% malicious node inducement, whereas the suggested model finds 79 packets. Finally, 30% of nodes are induced as malicious nodes, with the present model detecting 47 packets and the proposed method detecting 65.

Packet misclassification is a significant characteristic in terms of security since it analyzes incorrectly recognized packets, i.e., packets that may be truthful but are mistakenly recognized as hostile. As a result, the lower frequency of misclassified packets indicates a more efficient and appropriate model. The comparison of misclassified data packets is shown in Figure 5. Furthermore, when 10% of nodes are malevolent, the current model misclassifies 28 packets, but the suggested model only misclassifies 16. Likewise, the conventional model misclassifies 37 packets for 20% hostile nodes, whereas the suggested technique misclassifies 21 packets. Finally, in the presence of 30% hostile nodes, the current model detects 53 misclassified packets, but the proposed approach detects just 35.

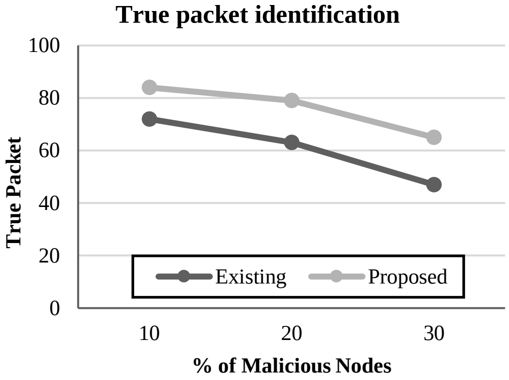

Figure 4. True packet comparison

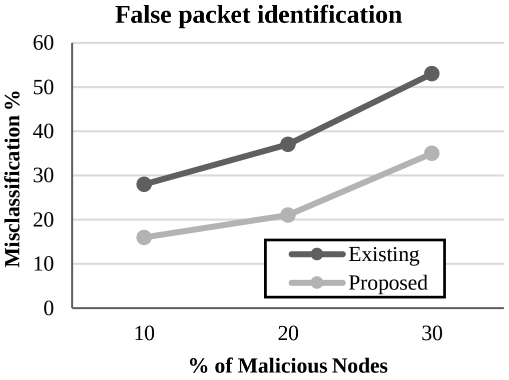

Figure 5. False packet identification

### 4.3. Model throughput

In general, throughput is measured as the rate at which the work is completed; the higher the throughput, the higher efficient the model is; Figure 6 compares the overall system throughput of the existing and suggested models. Furthermore, the conventional model detects a throughput of 0.612 for 10% malicious nodes, while the suggested model detects a throughput of 0.714. Furthermore, in the event of a 20% malicious node, the conventional model detects a throughput of 0.4788, whereas the suggested model detects a throughput of 0.604. Similarly, with 30% malicious nodes, the conventional model gets 0.2726 throughputs, but the proposed model gets 0.377.

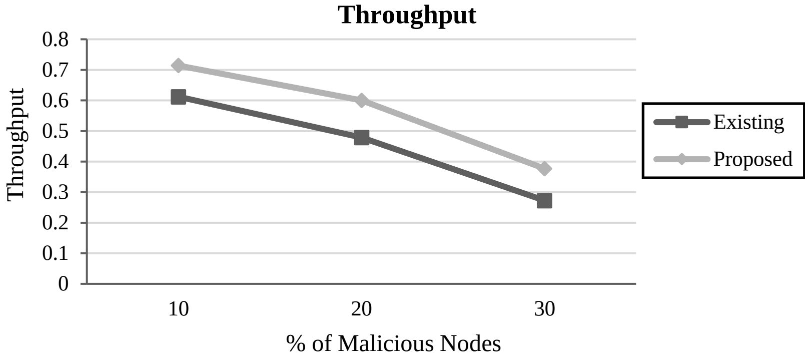

Figure 6. Model throughput

## 5. CONCLUSION

Data aggregation has been a fundamental module of the WSN environment in IoT applications; data aggregation has several benefits i.e., avoidance of data redundancy, parameter optimization, node functioning, and lifetime enhancement through energy utilization. However, it is obvious that WSNs are deployed in remote functions which makes the environment and network both vulnerable, thus it is required to have an efficient and secure model. Hence in this research article, we design and develop a DLI-security architecture that helps in efficiently providing secure data aggregation. The DLI-security architecture comprises two distinctive layers; the first layer comprises several sub-modules to establish the model's credibility and assure the establishment of secure communication among the nodes. In the second layer architecture, secure and efficient data aggregation is achieved through a consensus-based approach; also unsecured data packets are identified and removed from the network. Moreover, DLI-security architecture is evaluated considering parameters like energy by inducing the unsecured number of nodes; a comparison is carried out considering the true data packet identification and false data packet identification with the existing model. Although, DLI-security architecture possesses major advantages and marginal improvisation is observed while evaluating secure data aggregation; it is also to be noted that WSN environments are highly vulnerable, hence there is still scope for improvisation in the security model and different evaluation parameters should be considered further.

## REFERENCES

[1] S. Boubiche, D. E. Boubiche, A. Bilami, and H. Toral-Cruz, “Big data challenges and data aggregation strategies in wireless sensor networks,” *IEEE Access*, vol. 6, pp. 20558–20571, 2018, doi: 10.1109/ACCESS.2018.2821445.

[2] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, “An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs,” *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23826–23840, Dec. 2022, doi: 10.1109/JIOT.2022.3189832.

[3] S. Hu, L. Liu, L. Fang, F. Zhou, and R. Ye, “A novel energy-efficient and privacy-preserving data aggregation for WSNs,” *IEEE Access*, vol. 8, pp. 802–813, 2020, doi: 10.1109/ACCESS.2019.2961512.

[4] W.-K. Yun and S.-J. Yoo, “Q-learning-based data-aggregation-aware energy-efficient routing protocol for wireless sensor networks,” *IEEE Access*, vol. 9, pp. 10737–10750, 2021, doi: 10.1109/ACCESS.2021.3051360.

[5] A. Li, W. Liu, L. Zeng, C. Fa, and Y. Tan, “An efficient data aggregation scheme based on differentiated threshold configuring joint optimal relay selection in WSNs,” *IEEE Access*, vol. 9, pp. 19254–19269, 2021, doi: 10.1109/ACCESS.2021.3054630.

[6] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Jhanjhi, “Secure healthcare data aggregation and transmission in IoT-a survey,” *IEEE Access*, vol. 9, pp. 16849–16865, 2021, doi: 10.1109/ACCESS.2021.3052850.

[7] X. Li, T. Chen, Q. Cheng, S. Ma, and J. Ma, “Smart applications in edge computing: overview on authentication and data security,” *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4063–4080, Mar. 2021, doi: 10.1109/JIOT.2020.3019297.

[8] K. Xue, B. Zhu, Q. Yang, D. S. L. Wei, and M. Guizani, “An efficient and robust data aggregation scheme without a trusted authority for smart grid,” *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1949–1959, 2020, doi: 10.1109/JIOT.2019.2961966.

[9] Y. Lu, J. Li, and Y. Zhang, “Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted IIoT,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2553–2562, Apr. 2020, doi: 10.1109/JIOT.2019.2943379.

[10] S. Zhao *et al.*, “Smart and practical privacy-preserving data aggregation for fog-based smart grids,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 521–536, 2021, doi: 10.1109/TIFS.2020.3014487.

[11] C. Guo, P. Tian, and K.-K. R. Choo, “Enabling privacy-assured fog-based data aggregation in e-healthcare systems,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1948–1957, Mar. 2021, doi: 10.1109/TII.2020.2995228.

[12] X. Zuo, L. Li, H. Peng, S. Luo, and Y. Yang, “Privacy-preserving multidimensional data aggregation scheme without trusted authority in smart grid,” *IEEE Systems Journal*, vol. 15, no. 1, pp. 395–406, Mar. 2021, doi: 10.1109/JSYST.2020.2994363.

[13] I. F. Senturk, K. Akkaya, and S. Janansefat, “Towards realistic connectivity restoration in partitioned mobile sensor networks,” *International Journal of Communication Systems*, vol. 29, no. 2, pp. 230–250, Jan. 2016, doi: 10.1002/dac.2819.

[14] X. Wang, L. Xu, S. Zhou, and W. Wu, “Hybrid recovery strategy based on random terrain in wireless sensor networks,” *Scientific Programming*, pp. 1–19, 2017, doi: 10.1155/2017/5807289.

[15] Z. Mi, Y. Yang, and J. Y. Yang, “Restoring connectivity of mobile robotic sensor networks while avoiding obstacles,” *IEEE Sensors Journal*, vol. 15, no. 8, pp. 4640–4650, Aug. 2015, doi: 10.1109/JSEN.2015.2426177.

[16] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, “Privacy-preserving data aggregation computing in cyber-physical social systems,” *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 1, pp. 1–23, Jan. 2019, doi: 10.1145/3145625.

[17] Y. Chen, J.-F. Martinez-Ortega, L. Lopez, H. Yu, and Z. Yang, “A dynamic membership group-based multiple-data aggregation scheme for smart grid,” *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12360–12374, Aug. 2021, doi: 10.1109/JIOT.2021.3063412.

[18] X. Yan *et al.*, “Verifiable, reliable, and privacy-preserving data aggregation in FoG-assisted mobile crowdsensing,” *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14127–14140, Sep. 2021, doi: 10.1109/JIOT.2021.3068490.

[19] M. Zhang, H. Zhang, D. Yuan, and M. Zhang, “Learning-based sparse data reconstruction for compressed data aggregation in IoT networks,” *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11732–11742, Jul. 2021, doi: 10.1109/JIOT.2021.3059735.

[20] B. Yin and X. Wei, “Communication-efficient data aggregation tree construction for complex queries in IoT applications,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3352–3363, Apr. 2019, doi: 10.1109/JIOT.2018.2882820.

[21] C. H. Liu, Q. Lin, and S. Wen, “Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, Jun. 2019, doi: 10.1109/TII.2018.2890203.

[22] M. Du *et al.*, “Spacechain: A three-dimensional blockchain architecture for IoT security,” *IEEE Wireless Communications*, vol. 27, no. 3, pp. 38–45, Jun. 2020, doi: 10.1109/MWC.001.1900466.

[23] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, “A blockchain-based location privacy-preserving crowdsensing system,” *Future Generation Computer Systems*, vol. 94, pp. 408–418, May 2019, doi: 10.1016/j.future.2018.11.046.

[24] M. Li *et al.*, “CrowdBC: a blockchain-based decentralized framework for crowdsourcing,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 6, pp. 1251–1266, Jun. 2019, doi: 10.1109/TPDS.2018.2881735.

[25] S. Chen, Z. You, and X. Ruan, “Privacy and energy co-aware data aggregation computation offloading for fog-assisted IoT networks,” *IEEE Access*, vol. 8, pp. 72424–72434, 2020, doi: 10.1109/ACCESS.2020.2987749.

[26] R. waseem Anwar, A. Zainal, and S. Iqbal, “Systematic literature review on designing trust-based security for WSNs,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 14, no. 3, pp. 1395–1404, Jun. 2019, doi: 10.11591/ijeecs.v14.i3.pp1395-1404.

[27] A. S. Martey, E. Esenogho, and T. Swart, “Improved cluster to normal ratio protocol for increasing the lifetime of wireless sensor networks,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 26, no. 2, pp. 1135–1147, 2022.

[28] T. B. Seong, V. Ponnusamy, N. Zaman Jhanjhi, R. Annur, and M. N. Talib, “A comparative analysis on traditional wired datasets and the need for wireless datasets for IoT wireless intrusion detection,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 22, no. 2, pp. 1165–1176, May 2021, doi: 10.11591/ijeecs.v22.i2.pp1165-1176.

[29] M. Moshref, R. Al-Sayyed, and S. Al-Sharaeh, “Improving the quality of service in wireless sensor networks using an enhanced routing genetic protocol for four objectives,” *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 26, no. 2, pp. 1182–1196, May 2022, doi: 10.11591/ijeecs.v26.i2.pp1182-1196.

[30] G. B. Pallavi and P. Jayarekha, “Secure and efficient multi-tenant database management system for cloud computing environment,” *International Journal of Information Technology*, vol. 14, no. 2, pp. 703–711, Mar. 2022, doi: 10.1007/s41870-019-00416-5.

[31] G. Thahniyath and M. Jayaprasad, “Secure and load balanced routing model for wireless sensor networks,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 4209–4218, Jul. 2022, doi: 10.1016/j.jksuci.2020.10.012.

[32] J. Chang and F. Liu, “A byzantine sensing network based on majority-consensus data aggregation mechanism,” *Sensors*, vol. 21, no. 1, Jan. 2021, doi: 10.3390/s21010248.

[33] J. N. Al-Karaki and G. A. Al-Mashaqbeh, “SENSORIA: A new simulation platform for wireless sensor networks,” in *2007 International Conference on Sensor Technologies and Applications (SENSORCOMM 2007)*, Oct. 2007, pp. 424–429, doi: 10.1109/SENSORCOMM.2007.4394958.

## BIOGRAPHIES OF AUTHORS

**Rudramurthy Veeregowdanadoddi Chandraiah** received the B.E. degree in Information Science and Engineering and M.Tech. degree in Computer Science and Engineering from Visvesvaraya Technological University, Belagavi, Karnataka, India in 2004 and 2008 respectively. Currently, he is working as Assistant Professor at the Department of Computer Science and Engineering, Global Academy of Technology, Bengaluru. His research interests include wireless sensor networks and security. He can be contacted at email: rudramurthy.vc@gmail.com.

**Aparna Ramalingappa** holds a Ph.D from Visvesvaraya Technological University, Belagavi, Karnataka, India. Dr. R. Aparna is currently working as Professor in Department of Information Science and Engineering, Siddaganga Institute of Technology, Tumakuru, Karnataka, India. Her research areas are Cryptography and Network Security, Security in Wireless Sensor Networks, and Routing issues in Ad Hoc Wireless Networks. She has published more than 60 articles in various journals and conferences. She is having 3 book chapters. She can be contacted at email: raparna@sit.ac.in.