

Consensus-based secure and efficient compressive sensing in a wireless network sensors environment

Nandini S. Patil, Asma Parveen

Department of Computer Science and Engineering, Khaja Banda Nawaz College of Engineering, Kalaburagi, India

Article Info

Article history:

Received Jun 17, 2022

Revised Nov 12, 2022

Accepted Nov 18, 2022

Keywords:

Communication overhead

Compressive sensing

Compressive sensing

Consensus

Security

Wireless sensor network

ABSTRACT

Compressive sensing provides the optimal paradigm for data aggregation approach in wireless sensor networks as it holds the characteristics of low traffic cost and avoids the large communication overhead through a traditional approach. However, security is still considered one of the important, in recent years consensus-based approach has been one of the security highlights in compressive sensing. Moreover, a consensus is developed only with the help of genuine nodes. In this research work, a novel integrated-consensus-based secure compressive sensing (CSCS) is proposed which aims to develop a secure consensus environment to secure the network. Integrated-CSCS comprises several modules; at first certain variables are assigned to each node participating in the network. Later an algorithm is developed where each node evaluates the assigned neighbor variable and updates its states. Moreover, this phenomenon leads to the identification of genuine and compromised nodes. The proposed model is evaluated by considering the efficiency and security parameters; efficiency evaluation is carried out through energy consumption, and several node failures where as security is evaluated by considering the ability to identify the genuine node and malicious or corrupt node.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Nandini S. Patil

Department of Computer Science and Engineering, Khaja Banda Nawaz College of Engineering

Kalaburagi, Karnataka, India

Email: nandinipatil5@gmail.com

1. INTRODUCTION

The basis of the internet of things (IoT) is laid on the devices that are enabled to obtain an IP address for connection and communication via the internet. IoT has various applications in recent times in various fields. IoT is applied to our daily lives as the physical world has been interpreted digitally by the use of information [1]. Objects form a network in IoT that can process, transmit and sense useful information with the help of sensors that are a part of a wireless network sensors (WSN) over the years, WSN are the main part of any IoT model. The application of these networks combined with the latest technologies relating to IoT provides fast, economical as well as flexible applications. Wireless sensor networks have various applications for IoT where devices combined with the sensors are used for transmission of data avoiding human interference [2], [3]. Although, an issue is raised regarding the security of data transmission and requires constant attention and resolution of the problems that arises. These applications are deployed in various domains that include transportation, the healthcare industry, and education [4]. The main aim of these sensory node functions is the monitoring and reporting of data that is collected for the base station. Therefore, this reduces the consumption of energy while the data is being communicated among the nodes; this is a trending topic over the years. Recent studies have proven that the architectural structure resolves the issues of transmission of data along with the efficiency of energy as well as an extended lifetime of the network of wireless sensors [5]-[7].

Presently, the devices that are used for sensing are deployed for IoT services. These devices used for sensing are deployed extensively for various activities throughout that lessen the burden on humans and reduce labour. The count on these devices has crossed that of humans and is further increasing rapidly [8], [9]. The advancements in technology relating to microprocessors focus on the storing and computing of these devices that have been enhanced. The technologies used today for a simple Smartphone can be compared to that of a computer 10 years back, such are the advancements in technology [10]. Although, the growth of the technology related to these sensory devices is increasing the size of these devices has decreased with time making them more compatible and efficient for their use in various domains [11]. The technologies and model of the network architecture have undergone various changes over the years about computing calculations for fog [12] and edge computing [13], [14] as well as the shift from centre to decentralization of the network architecture [15]. The WSN is an integral part of the network that includes nodes that are self-organized as well as had a multi-hop structure that is combined to receive valuable information for the area and send the information to the related applications. The applications of this network are across various domains that include agriculture, transportation, infrastructure, military, traffic, industries, and ecological applications. Wireless networks in these domains are used in various ways, in agriculture, the yield and growth of the crops can be monitored using these networks. The traffic can be controlled by constant monitoring of the traffic patterns, military applications involving harsh environmental conditions on battlefields [16]-[18].

These wireless networks are also deployed in critical conditions where hazardous environmental conditions; these circumstances include battery-powered energy making it difficult to restore [19]. This causes the energy that is used by these networks to become limited. Hence, it is of the utmost concern to focus research on extending the energy life of this network [20].

The proposed work in this paper aims at compressive sensing theory for a novel sampling signal that is used to decrease the transmitted data from the nodes and is well suited for wireless networks that include sensors. The main aim of this paper is the recovery of a signal that is of finite dimension from a smaller linear measurement set for a sparse signal at the base. Considering a method for the usual collection of data, the network has nodes n , which have data readings $W = [w_1, w_2, w_3 \dots w_h, \dots w_n]$. In this case, w_h is the reading of the data at the sensor h . We consider the non-compressive theory of sense, where the quantity of data from every node is required to process through a route that is multi-hop to get to the sink. For this type of collection of data, the quantity of data that is taken up by the sink node that is far is considered to be small and the sensor that is within a single hop close to the sink has to send the entire node data of the wireless network. This infers that there are n packets of data that cause the node that is in the range of the closest sink. The quantity of data that is processed is large and is termed the hotspots of the area. Considering the compressive sensing theory, the network has used the perceptual theory; in this, the sensor is required to transmit a value of observation that is of m -dimension. The quantity of the data for every node has m number of packets. In comparison to the non-compressive sensing theory, the highest quantity of data for the nodes is noticeably decreased which in turn extends the life of the network.

A. Motivation and contribution of the research

The data involves plain text files, images of various sizes and formats as well as multimedia files. The transmission of data over the channel of communication without the main task being disclosed. The network with a multi-node system consists of various malicious nodes that corrupt the other nodes or could corrupt the information that is being transmitted. It is essential to bifurcate the malicious nodes from the uncorrupted nodes for the secure transmission of data without any threat to the network as well as without any loss of data in the network. Furthermore, the contribution of this proposed work is as given below:

- a) A data compressive sensing methodology is proposed for a secure multi-node system with the detection of compromised nodes as well as uncorrupted nodes.
- b) A consensus is proposed for the bifurcation or detection of malicious or corrupt nodes while the transfer of data occurs. While the direction of the transfer is also explained by utilizing a directed graph.
- c) An algorithm is a propose algorithm for the compression sensing to be performed at time t while considering that the information being transferred is correct.
- d) We proposed an algorithm for the compression sensing to be performed at time t while considering the information that is communicated to be noise in the network.

This particular research work is organized as follows: the section 1 starts with the background of IoT devices and wireless networks with sensors along with security concerns of the nodes in the network while considering a multi-node system. Further, the same section discusses the related work of existing models along with their shortcomings. The section 1 ends with research motivation and contribution of research work. The section 2 proposes a compressive sensing algorithm along with the proposed architecture and mathematical model. The section 3 evaluates the model by comparing it with the existing model.

2. RELATED WORK

The emergence of distributed compressive sensing (CS) has led to several researches paying attention to the CS technology in the WSN environment. Further, a recent discussion on the adoption of CS in WSN applications has raised an eyebrow due to security concerns. Hence this section of the research focuses on reviewing a few related works.

Guo *et al.* [21], a mechanism is proposed that focuses on the privacy preservation of the compressive sensing that is applied for road traffic networks considering a period with various conditions applied as well as a design for a flexible and secure protocol for computing the rate of processing the data. Especially during the use of the cloud for retrieving the temporal and spatial correlation between various parts of the road and computation of the roads that have excessive traffic congestion. A compressive sensing mechanism is proposed in the paper to calculate the traffic on the roads considering its conditions based on a few values that are known. Qi *et al.* [22], a scheme is proposed for the security of compressive sensing applied to multimedia sensors with data. The mechanism proposed in this paper is light security, which therefore reduces the energy that is consumed. There is a detailed analysis of the performance that focuses on compression as well as security. Salim *et al.* [23], the proposed work consists of three distinct and important phases. The first phase is the setup phase in which the characteristics of prime numbers are introduced for clustering as well as an algorithm for routing, both of which are used to consume power at the time of transmission of data. The second phase of the proposed work includes the security of data for communication within and outside the network. The communication within the network uses compressive sensing for the compression of data as well as encryption. The third phase of this work is the reconstruction of data. Yuan *et al.* [24], a joint clustering route for gathering data based on compressive sensing is proposed in this paper. This is used to improvise and extend the lifetime of the network. The main technology that is adopted in this work is the collection of data performed by clustering. The network is initially formed as a cluster in which every node of the cluster has packets of data that are sent to the head of the cluster. Every cluster is an m -dimension of data considering the required methodology used to be compressive sensing. This is utilized to ensure that the data in this system can be recoverable. Unde and Deepthi [25], a compressive sensing system is proposed for efficient and effective encryption by the use of switched reluctance machine (SRM) for IoT devices that are multimedia. The attenuation is artificially introduced in the compressive sensing technology for the resistance of CPA, this is performed for the analysis of the distortion rate of the compressive sensing. Ketshabetswe *et al.* [26] a comparative study is performed on the methodologies used in the compression of data for networks that include wireless sensors. An algorithm for compression of data without the loss of data is adapted and analysed under MATLAB to discover the methods that can be utilized to decrease the data that is being transferred.

3. PROPOSED METHODOLOGY

Recently, the emerging area of CS provides a new perspective for data acquisition and processing in WSNs, which enables source compression to be performed with low-complexity sensor nodes. Compressive sensing provides a new paradigm for signal acquisition and processing. According to the theory of CS, a sparse or compressible signal can be reconstructed with high probability from a small number of measurements, which is far smaller than the length of the original signal. In this research work, we present an Integrated-consensus-based secure compressive sensing (CSCS) mechanism that aims at securing the network and smooth data transmission.

We assume a system consisting of multiple nodes, this system is made up of M number of nodes and the model having h^{th} node is given as (1).

$$w_h s + w_h = Z w_h(s) + A t_h(s) \quad (1)$$

Considering the (1), w_h belongs to Q^m which is a vector that can be measured. Z belongs to $Q^{m \times m}$ are the matrix and A belongs to $Q^{m \times 1}$ is the matrix input in the equation. The t_h belongs to Q which is the input control.

State : Consider (Z, A) can be controlled for which a similar expression is used as (2).

$$\vartheta_h(s) = \frac{w_h(s)}{s} \quad \text{where;} \quad \det(yH_m - Z) = y^m + \varphi_1 y^{m-1} + \varphi_2 y^{m-2} + \dots + \varphi_m \quad (2)$$

The multiple nodes system that is given using (1) is expressed as a model for a companion as (3).

$$\vartheta_h(s + 1) = \bar{Z}\vartheta_h(s) + \bar{A}t_h(s) \tag{3}$$

Considering (3) we were given the following matrix expression that gives the value of \bar{Z} and \bar{A} .

$$\bar{Z} = \begin{bmatrix} -\varphi_1 & -\varphi_2 & \dots & -\varphi_{m-1} & -\varphi_m \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{bmatrix} \text{ and } \bar{A} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

We use this matrix expression for the final evaluation of the proposed work. The attacks that are done by the nodes that are suspected do show some signs of behaviour that appear to be malicious. These nodes are considered to be malicious nodes in the system, but there occurs a criterion to term them as malicious nodes. The nodes are termed malicious nodes only if they exhibit the following properties: (1) The states of these nodes are improvised or upgraded in a way that breaches the protocol to be followed that is designed for the system. In (2) The information or data that is communicated in the network is incorrect and different from the original data that is being shared.

In the multi-node system, there consist various nodes that interact with each other this interaction communication is expressed in the form of a graph with direction as $G = (U, \omega, Z)$ in which the nodes M is given as $U = \{1, 2, \dots, M\}$ and ω is the links of communication or interaction between the various nodes such that $\subseteq U \times U$. The sending node and the receiving node are (i, h) respectively meaning that the h^{th} node receives data that is sent from the i^{th} node. This shows that both the nodes that send and receive information are neighbours. Therefore, we define \mathbb{N}_h as the neighbouring set of nodes that are concerning node h . We also express the adjacent matrix to the graph G as \mathcal{A} which is given as $\mathcal{A} = [z_{h,i}]$ which belong to $\mathcal{R}^{M \times M}$ in which $[z_{h,i}]$ belongs to $\mathcal{R}_{>0}$ only when (i, h) belongs to ω , i does not equal h and is otherwise zero. The node weight between the two nodes is determine by the calculation of $z_{h,i}$. These calculations are considered while the protocol for malicious nodes is being framed. Considering a graph with direction G , has a set that is not null and is reachable (r) such that $|\mathbb{N}_h \setminus R|$ is greater than or equal to r . The graph G is also termed as robust (r) when two sets are not null and are disjoint such that the two sets are a subset of U and the intersection of the two sets is a null, during which at least one of the sets are reachable. However, the nodes of set $R \subset U$ are termed as focal points *local - f*.

We proposed a scheme for compressive sensing considering the interaction failure among the nodes. We propose a criterion that ensures security in the network for which the nodes that are honest and uncorrupted remain within the network limits. In this system, the h^{th} node of the network has a safety constant $r_h(s)$ among the various other nodes. This constant has to be evaluated for its value by the i^{th} node that also is uncorrupted, which selects the node for communication. When fails to do so it follows, (*if h belongs to $\mathbb{N}_h(o)$, i belongs U_g*). If an uncorrupted node selects the h^{th} node for communication, in which case the $r_h(s)$ is utilized for a compressive sensing protocol by that node which results in consensus eventually in the system. Every node in the network upgrades itself at specified periods based on the safety constant of the neighbouring nodes without hindering its security and safety. Hence, there are constraints for breaking the links for communication in the network of nodes, which include a stochastic failure among the node links during communication and when an uncorrupted node ignores the links of communication from some neighbouring nodes. For this case, we define the proposed constant $j_{h,i}(s)$, h belongs to U_h , i belongs to $\mathbb{N}_h(o)$ for which $j_{h,i}(s)$ equals 1. This is used to define the h^{th} node of the network that chooses the i^{th} node which is its neighbour and $j_{h,i}(s)$ is equal to zero if this condition is not satisfied.

After the process of selection or ignoring is performed it is essential to express the effectiveness of the network concerning the matrix that is adjacent, given as $Z(o, s) = [z_{h,i}(o, s)]$ where the value of $z_{h,i}(o, s)$ is defined as it belongs to $Q_{>0}$ when $o_{h,i}(s)$ and $j_{h,i}(s) = 1$. it is equal to 0 when $1 - o_{h,i}(s)$ and $j_{h,i}(s) = 0$. Similarly, the set of neighbouring nodes that are effective for every node is defined as $\mathbb{N}_h(o, s)$. It is also assumed that these malicious nodes are not within the control of the network and therefore, the entry of the matrix that is adjacent is not of importance or value to the network. After the selection of the neighbouring nodes that are secure, a strategic scheme should be proposed so that it ensures the consensus is carried out to the nodes that are uncorrupted and also ensures the safety constants of the uncorrupted nodes. Hence, a framework is proposed that consists of two-phase to control the nodes that are uncorrupted.

3.1. First phase

Consider an uncorrupted node h that has input or received the data $r_i(s)$, when the sending node i belongs to $\mathbb{N}_h(o)$ then the value of $j_{h,i}(s)$ is set to 1. When $|\mathbb{N}_h(o)|$ is greater than or equal to e , then all the neighbouring nodes of e have the largest data or information and if $|\mathbb{N}_h(o)|$ is less than e , then we take into consideration all the neighbours of $|\mathbb{N}_h(o)|$. Considering the neighbours of the node i , if the information

or data from node i is greater than the information or data from node h , in this case $j_{h,i}(s)$ is equal to 0. When $|\mathbb{N}_h(o)|$ is greater than or equal to e , then neighbours of e have the smallest data of the node i . For a neighbouring node i , the information of node i is greater than the information of the node h , in this case $j_{h,i}(s)$ is equal to 0. Because the binding of the node information $r_h(s)$ which has to ensure the binding of the uncorrupted nodes state by (4).

$$\vartheta_h(s) = [\vartheta_{m-1,h}(s)\vartheta_{m-2,h}(s) \dots \vartheta_{0,h}(s)] \quad (4)$$

The proposed method in this paper is evaluated using the above equation as (5).

$$r_h(s) = \vartheta_{m-1,h}(s) + \sum_{l=0}^{m-1} \vartheta_{m-1,h}(s)\beta_l \quad (5)$$

Considering the above equation, h belongs to U_g , in which $\beta_1, \beta_2, \dots, \beta_{m-1}$ belongs to \mathcal{R} such that the polynomial forms a sequence as (6).

$$\text{polynomial}(y) = y^{m-1} + \beta_1 y^{m-2} + \beta_3 y^{m-3} + \dots + \beta_{m-1} \quad (6)$$

3.2. Second phase

A methodology is designed for the compressive sensing consensus by the utilization of information from the neighbouring nodes that are mentioned above. In addition, by emphasizing the constraints of selecting the neighbouring nodes, the uncorrupted nodes are transmitted securely. We proposed an algorithm for the compressive sensing to be performed at time t . Listed below are the steps of the proposed algorithm 1.

Algorithm 1. Compressive sensing to be performed at time t

- Step 1 Data $r_i(s)$ is received by the uncorrupted node h
 Step 2 Evaluation
 When node h belongs to $\mathbb{N}_h(o)$ then $j_{h,i}(s) = 1$
 Step 3 When $\mathbb{N}_h(o)$ is greater than or equal to e ,
 We consider the neighbouring nodes of e with the largest data $r_i(s)$
 When $\mathbb{N}_h(o)$ is lesser than e ,
 We consider all the neighbours of $\mathbb{N}_h(o)$
 Step 4 If $r_i(s) > r_h(s)$ then $j_{h,i}(s) = 0$
 Step 5 When $\mathbb{N}_h(o)$ is greater than or equal to e ,
 We consider the neighbouring nodes of e with the smallest data $r_i(s)$
 When $\mathbb{N}_h(o)$ is lesser than e ,
 We consider all the neighbours of $\mathbb{N}_h(o)$
 Step 6 If $r_i(s) < r_h(s)$ then $j_{h,i}(s) = 0$
 Step 7 Evaluation of the adjacent matrix for effective entry of $z_{h,i}(o,s)$ by $j_{h,i}(s)$, where the nodes upgrade their state through the proposed protocol for interaction and communication.

We proposed an algorithm for the compressive sensing to be performed at time t while considering the information that is communicated to be noise in the network. Listed below are the steps of the proposed algorithm.

Algorithm 2. Algorithm for compressive sensing for attenuated data

- Step 1 Attenuated Data $\tilde{r}_{h,i}(s)$ is received by the uncorrupted node h .
 Step 2 Evaluation
 When node h belongs to $\mathbb{N}_h(o)$ then $j_{h,i}(s,\rho) = 1$
 Step 3 When $\mathbb{N}_h(o)$ is greater than or equal to e ,
 We consider the neighbouring nodes of e with the largest data $\tilde{r}_{h,i}(s)$
 When $\mathbb{N}_h(o)$ is lesser than e ,
 We consider all the neighbours of $\mathbb{N}_h(o)$
 Step 4 If $\tilde{r}_{h,i}(s) > r_h(s)$ then $j_{h,i}(s,\rho) = 0$
 Step 5 When $\mathbb{N}_h(o)$ is greater than or equal to e ,
 We consider the neighbouring nodes of e with the smallest data $\tilde{r}_{h,i}(s)$
 When $\mathbb{N}_h(o)$ is lesser than e ,
 We consider all the neighbours of $\mathbb{N}_h(o)$
 Step 6 If $\tilde{r}_{h,i}(s) < r_h(s)$ then $j_{h,i}(s,\rho) = 0$
 Step 7 Evaluation of the adjacent matrix for effective entry of $z_{h,i}(o,s,\rho)$ by $j_{h,i}(s,\rho)$, where the nodes upgrade their state through the proposed protocol for interaction and communication.

4. PERFORMANCE EVALUATION

Compressive sensing is considered one of the optimal data aggregation approach as it exceeds the other traditional approach to the issue of communication overhead and low traffic cost. The main intention of CS is to minimize energy consumption and increase the network lifetime. This section of the research evaluates the proposed approach of secure compressive sensing; moreover, the proposed methodology is evaluated by inducing the insecure nodes (here insecure node indicates that by default it is made as to the corrupt node). The proposed secure compressive sensing approach is evaluated under the described system configuration, which includes 2 TB of the hard disk loaded with 16 GB of RAM along with 2 GB NVidia CUDA-enabled graphics. The proposed model is evaluated by inducing the compromised node which aims to create an imbalance in the network by compromising the different security aspects; compromised nodes induced are 5, 10, 15, and 20. Also other parameters like energy number of dead nodes, delay are considered for the evaluation as it gets affected through network imbalance. Further, a comparative analysis is carried out with the existing model to ensure the model's security and efficiency.

4.1. Energy utilization

Energy is considered one of the major parameters for efficiency evaluation in WSN led IoT environment. Figure 1 shows the average energy utilized to perform the simulation for various compromised nodes. In the case of 5 compromised nodes, the average energy required is 3.63 MJ, for 10 compromised nodes, the average energy required is 3.58 MJ. Similarly, for 15 and 20 compromised nodes, the energy required is 3.53 MJ and 3.51 MJ respectively.

4.2. Correct node identification

This section presents the comparison of the proposed and existing model considering the identification of genuine nodes while inducing the compromised nodes as 5, 10, 15, and 20 nodes. Figure 2 shows the comparison of it; In the case of five compromised nodes, the existing model identifies 98 correct nodes whereas the proposed model identifies all the nodes. Similarly, for 10 compromised nodes, the existing model identifies 91 nodes whereas the proposed model identifies 100 nodes. In the case of 15 and 20 compromised nodes, the Existing model identifies 91 and 87 whereas the proposed model identifies 98 and 91 respectively.

4.3. Wrong identification

Figure 3 shows the wrong identification of nodes, for 5 and 10 compromised nodes. The existing model identifies 3 and 10 wrong nodes respectively whereas the proposed model does not misclassify for 5 compromised nodes and wrongly identified a single node for 10 compromised nodes. In the case of 15 and 20 nodes, the existing model wrongly identifies 10 and 14 nodes respectively whereas the proposed model wrongly identifies 3 and 10 nodes respectively.

4.4. Comparative analysis and discussion

This section presents the comparative analysis by presenting the improvisation over the existing model. Figure 4 shows the proposed model improvisation. Improvisation is evaluated on correct and incorrect identification; in the case of five compromised nodes, integrated-CSCS observes 3.06% improvisation and 100% improvisation in incorrect identification. Similarly, for 10 and 15, integrated-CSCS observes 9.89% for correct identification and 90% for improvisation in misidentification.

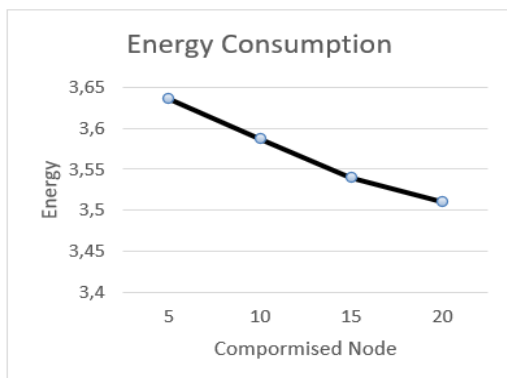


Figure 1. Correct node identification

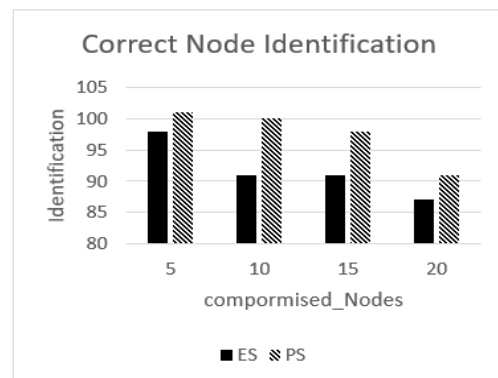


Figure 2. Energy consumption

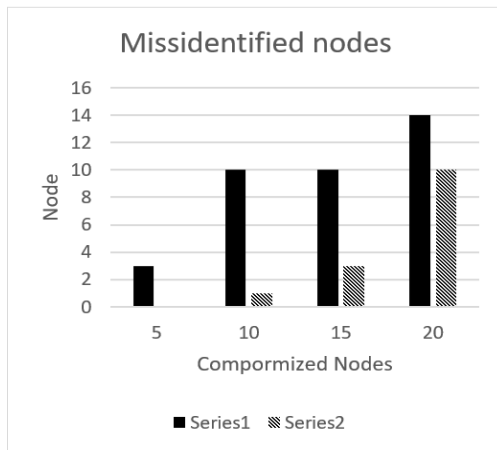


Figure 3. Miss identified nodes

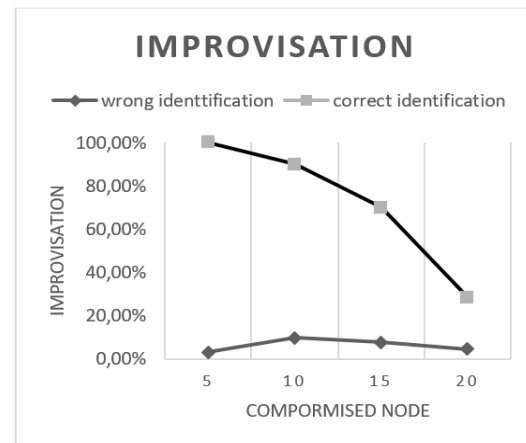


Figure 4. Improvisation

5. CONCLUSION

Collecting the data is the main objective of WSN and it is one of the bases for different applications in the WSN environment. Moreover, data collection has different categories such as event-driven, query-driven, and time-driven based on the application. Compressive sensing is one of the optimal approaches that avoid the issues of different categories; along with optimal aggregation, the important part is to secure the compressive sensing approach. In this research work, integrated-CSCS is proposed for securing the compressive sensing approach; in this, each sensor is assigned a certain variable and an algorithm is designed to evaluate the assigned variable concerning neighbours. Moreover, integrated-CSCS is evaluated considering the secure and efficient parameter through inducing the different compromised nodes. In the case of 5, 10, 15, and 20 compromised nodes, integrated-CSCS achieves improvisation of up to 10% for correct identification and it achieves up to 100%. Further, integrated-CSCS observes 2.15%, 11.11%, 7.79%, and 4.34% for 5, 10, 15, and 20 compromised nodes. Although integrated-CSCS achieves optimal security along with efficiency, considering the network complexity and rise of machine learning-based attacks in-network, other security parameters should be evaluated.




REFERENCES

- [1] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," in *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182-8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.
- [2] N. A. M. Alduais, J. Abdullah, and A. Jamil, "RDCM: An efficient real-time data collection model for IoT/WSN edge with multivariate sensors," in *IEEE Access*, vol. 7, pp. 89063-89082, 2019, doi: 10.1109/ACCESS.2019.2926209.
- [3] J. Liu, Z. Zhao, J. Ji, and M. Hu, "Research and application of wireless sensor network technology in power transmission and distribution system," in *Intelligent and Converged Networks*, vol. 1, no. 2, pp. 199-220, Sept. 2020, doi: 10.23919/ICN.2020.0016.
- [4] M. Frustaci, P. Pace, G. Aloï, and G. Fortino, "Evaluating critical security issues of the IoT world: present and future challenges," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483-2495, Aug. 2018, doi: 10.1109/JIOT.2017.2767291.
- [5] K. Yang, Q. Yu, S. Leng, B. Fan, and F. Wu, "Data and energy integrated communication networks for wireless big data," in *IEEE Access*, vol. 4, pp. 713-723, 2016, doi: 10.1109/ACCESS.2016.2526622.
- [6] Y. Wang, K. Yang, W. Wan, Y. Zhang, and Q. Liu, "Energy-efficient data and energy integrated management strategy for IoT devices based on RF energy harvesting," in *IEEE Internet of Things Journal*, vol. 8, no. 17, pp. 13640-13651, 1 Sept. 1, 2021, doi: 10.1109/JIOT.2021.3068040.
- [7] Z. Guo *et al.*, "Minimizing redundant sensing data transmissions in energy-harvesting sensor networks via exploring spatial data correlations," in *IEEE Internet of Things Journal*, vol. 8, no. 1, pp. 512-527, 1 Jan. 1, 2021, doi: 10.1109/JIOT.2020.3004554.
- [8] L. Nkenyereye, J. Hwang, Q.-V. Pham, and J. Song, "Virtual IoT service slice functions for multiaccess edge computing platform," in *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11233-11248, 2021, doi: 10.1109/JIOT.2021.3051652.
- [9] T. Zhang, J. Jin, X. Zheng, and Y. Yang, "Rate-adaptive fog service platform for heterogeneous IoT applications," in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 176-188, Jan. 2020, doi: 10.1109/JIOT.2019.2945328.
- [10] J. M. Vicente-Samper, E. Ávila-Navarro, and J. M. Sabater-Navarro, "Data acquisition devices towards a system for monitoring sensory processing disorders," in *IEEE Access*, vol. 8, pp. 183596-183605, 2020, doi: 10.1109/ACCESS.2020.3029692.
- [11] Z. Song, Z. Cao, Z. Li, J. Wang, and Y. Liu, "Inertial motion tracking on mobile and wearable devices: Recent advancements and challenges," in *Tsinghua Science and Technology*, vol. 26, no. 5, pp. 692-705, Oct. 2021, doi: 10.26599/TST.2021.9010017.
- [12] N. Nesa and I. Banerjee, "SensorRank: an energy efficient sensor activation algorithm for sensor data fusion in wireless networks," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2532-2539, April 2019, doi: 10.1109/JIOT.2018.2871469.
- [13] Jia, H. Hu, Y. Zeng, T. Xu, and Y. Yang, "Double-matching resource allocation strategy in fog computing networks based on cost efficiency," in *Journal of Communications and Networks*, vol. 20, no. 3, pp. 237-246, June 2018, doi: 10.1109/JCN.2018.000036.




- [14] M. D. Donno, K. Tange, and N. Dragoni, "Foundations and evolution of modern computing paradigms: Cloud, IoT, edge, and fog," in *IEEE Access*, vol. 7, pp. 150936-150948, 2019, doi: 10.1109/ACCESS.2019.2947652.
- [15] M. Goudarzi, H. Wu, M. Palaniswami, and R. Buyya, "An application placement technique for concurrent IoT applications in edge and fog computing environments," in *IEEE Transactions on Mobile Computing*, vol. 20, no. 4, pp. 1298-1311, 2021, doi: 10.1109/TMC.2020.2967041.
- [16] S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, "Soft-WSN: Software-defined WSN management system for IoT applications," in *IEEE Systems Journal*, vol. 12, no. 3, pp. 2074-2081, Sept. 2018, doi: 10.1109/JSYST.2016.2615761.
- [17] G. Yildirim and Y. Tatar, "Simplified agent-based resource sharing approach for WSN-WSN interaction in IoT/CPS projects," in *IEEE Access*, vol. 6, pp. 78077-78091, 2018, doi: 10.1109/ACCESS.2018.2884741.
- [18] Thomas, R. Shankaran, M. A. Orgun, and S. C. Mukhopadhyay, "SEC2: A secure and energy efficient barrier coverage scheduling for WSN-based IoT applications," in *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 622-634, 2021, doi: 10.1109/TGCN.2021.3067606.
- [19] O. Said, Z. Al-Makhadmeh, and A. Tolba, "EMS: An energy management scheme for green IoT environments," in *IEEE Access*, vol. 8, pp. 44983-44998, 2020, doi: 10.1109/ACCESS.2020.2976641.
- [20] O. Said, Y. Albagory, M. Nofal, and F. Al Raddady, "IoT-RTP and IoT-RTCP: Adaptive protocols for multimedia transmission over internet of things environments," in *IEEE Access*, vol. 5, pp. 16757-16773, 2017, doi: 10.1109/ACCESS.2017.2726902.
- [21] W. Guo, J. Li, X. Liu, and Y. Yang, "Privacy-preserving compressive sensing for real-time traffic monitoring in Urban City," in *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14510-14522, Dec. 2020, doi: 10.1109/TVT.2020.3042794.
- [22] J. Qi, X. Hu, Y. Ma, and Y. Sun, "A hybrid security and compressive sensing-based sensor data gathering scheme," in *IEEE Access*, vol. 3, pp. 718-724, 2015, doi: 10.1109/ACCESS.2015.2439034.
- [23] A. Salim, W. Osamy, A. M. Khedr, A. Aziz, and M. Abdel-Mageed, "A secure data gathering scheme based on properties of primes and compressive sensing for IoT-based WSNs," in *IEEE Sensors Journal*, vol. 21, no. 4, pp. 5553-5571, 2021, doi: 10.1109/JSEN.2020.3032585.
- [24] Y. Yuan, W. Liu, T. Wang, Q. Deng, A. Liu, and H. Song, "Compressive sensing-based clustering joint annular routing data gathering scheme for wireless sensor networks," in *IEEE Access*, vol. 7, pp. 114639-114658, 2019, doi: 10.1109/ACCESS.2019.2935462.
- [25] A. S. Unde and P. P. Deepthi, "Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia IoT," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67, no. 1, pp. 167-171, Jan. 2020, doi: 10.1109/TCSII.2019.2897839.
- [26] K. L. Ketshabetswe, A. M. Zungeru, B. Mtengi, C. K. Lebekwe, and S. R. S. Prabakaran, "Data compression algorithms for wireless sensor networks: A review and comparison," in *IEEE Access*, vol. 9, pp. 136872-136891, 2021, doi: 10.1109/ACCESS.2021.3116311.

BIOGRAPHIES OF AUTHORS



Nandini S. Patil    received the B.E & M.Tech. degree in computer science & engineering from VTU University, Belgaum. She is pursuing Ph.D. in Khaja Banda Nawaz college of Engineering Kalaburagi. The area of Interest is WSN and IoT. She can be contacted at email: nandinipatil5@gmail.com.



Dr. Asma Parveen    is Presently working as Assoc. Prof. at KBN College of Engineering, Kalaburagi. She completed Ph.D. degree in computer science and Engineering. She recieved M.Tech. and B. E. degree in CSE from VTU, Belgaum. The area of Interest is networking, IoT, and machine learning. She can be contacted at email: drasma.cse@gmail.com.