

Enhanced Cyber Physical Security Based Automatic Generation Control with Renewable Energy System

Rajkamal M¹, Swathi D², Prabu S³, Mohanapriya P⁴, Sumathi.M⁵

¹Application Developer, IBM, Bangalore,

²Assistant Professor, K.Ramakrishnan College of Engineering, Samayapuram, Trichy.

³Research Scholar, SASTRA University, Thanjavur,

⁴Software Engineer, Hexaware Technologies Ltd, Chennai.

⁵Assistant Professor, K.Ramakrishnan College of Engineering, Samayapuram, Trichy.

Email: sumathishanjai.nitt@gmail.com

Abstract:

Photovoltaic (PV) systems are becoming more vulnerable to cyber threats. Developing cyber-secure power electronics converters has received increased attention from the IEEE power electronics society (PELS) that recently launched a cyber-physical-security initiative. The multilayer long short-term memory networks (MLSTM) are used to leverage time-series electric waveform data from current and voltage sensors in PV systems. Comparison results verify performances of the proposed method for detection and diagnosis of various data integrity attacks on PV systems.

Keywords: Photo-voltaic, Power Electronic Society, Multilayer Long Short-Term Memory.

I. Introduction

The term wireless communication was introduced and has developed over the subsequent years. It is one of the most important mediums of transmission of information from one device to other devices. In this technology, the information can be transmitted through the air without requiring any cable or wires or other electronic conductors, by using electromagnetic waves like IR, RF, satellite, etc. [1]. In the present days, the wireless communication technology refers to a variety of wireless communication devices and technologies ranging from smart phones to computers, tabs, laptops, Bluetooth Technology, etc. The various types of wireless communication include satellite communication, infrared communication, broadcast radio etc. The major advantages are cost effectiveness, flexibility, convenience, speed, accessibility and constant connectivity [2].

Wideband jamming can be used to reduce the effectiveness of spread spectrum techniques by jamming over a wide range of communication channels, but this increased impact requires

significantly more energy than narrowband jamming. A certain jamming technique may be more suited to denying service to a wireless access point, while another may be able to accurately target primary communication systems [3]. Finally, the adversary's degree of reluctance towards being detected and subsequently prosecuted will determine to what extent a flight crew alarm could be used as a deterrent. The interaction between the aircraft network and the jammers, we set up a two-player jamming game. Game theory allows for succinct representation of a diverse array of network and jammer types, goals, and actions and is useful in modelling their interactivity [4].

The remaining sections of this article are organized as follows. In section 2, the works that are related to wireless communication technique with jammer attack is discussed with its merits and issues. Section 3, our proposed system is discussed with system architecture and necessary algorithms in a detail manner. In section 4, the proposed technique experimental results are discussed with existing work. Finally in section 5, the proposed work is concluded with its future enhancements.

II. Related Works

In this work the physical layer security for heterogeneous networks (HetNets) is investigated, where the confidential message transmitted to each legitimate user can be eavesdropped by multiple eavesdroppers. To enhance the secrecy performance, the friendly jammers and full duplex users is introduced. The proposed jammer selection scheme based on average user received jamming power. The jammers whose interference power on the scheduled users less than a threshold are selected to transmit independent artificial noise to confound the passive eavesdroppers [5]. Furthermore, the scheduled users try to jam the eavesdroppers around using full duplex capacity. Using the tools from stochastic geometry and derived the theoretical analyses of user connection probability and secrecy probability. In particular, the locations of selected jammers are modelled by a Poisson hole process instead of more popular homogeneous Poisson point process. The analytical results show a good agreement with the simulations. The ergodic secrecy rate in our scheme outperforms that in the traditional HetNets [6].

The situation in which digital data is to be reliably transmitted over a discrete, memory-less channel (DMC) that is subjected to a wire-tap at the receiver. Assume that the wire-tapper views the channel output via a second DMC). Encoding by the transmitter and decoding by the receiver are permitted. However, the code books used in these operations are

assumed to be known by the wire-tapper [7]. The designer attempts to build the encoder-decoder in such a way as to maximize the transmission rate R , and the equivocation d of the data as seen by the wire-tapper. The trade-off curve between R and d , assuming essentially perfect ("error-free") transmission is analysed. In particular, if d is equal to H_s , the entropy of the data source, then the transmission is accomplished in perfect secrecy. The experimental results implied that there exists a $C_s > 0$, such that reliable transmission at rates up to C_s is possible in approximately perfect secrecy [8].

The simultaneous wireless information and power transfer (SWIPT) in orthogonal frequency division multiple access (OFDMA) systems with the coexistence of information receivers (IRs) and energy receivers (ERs). The IRs was served with best-effort secrecy data and the ERs harvest energy with minimum required harvested power. To enhance the physical layer security for IRs and yet satisfy energy harvesting requirements for ERs and a new frequency-domain artificial noise (AN) aided transmission strategy is proposed [9]. With the new strategy, the optimal resource allocation for the weighted sum secrecy rate maximization for IRs by power and subcarrier allocation at the transmitter is analysed. The analysed problem is shown to be a mixed integer programming problem and thus non-convex, than the efficient algorithm for solving it based on the Lagrange duality method. To further reduce the computational complexity, the proposed a suboptimal algorithm of lower complexity. The simulation results illustrate the effectiveness of proposed algorithms as compared against other heuristic schemes [10].

Due to the broadcast nature of radio propagation, the wireless air interface is open and accessible to both authorized and illegitimate users. This completely differs from a wired network, where communicating devices are physically connected through cables and a node without direct association is unable to access the network for illicit activities. The open communications environment makes wireless transmissions more vulnerable than wired communications to malicious attacks, including both the passive eavesdropping for data interception and the active jamming for disrupting legitimate transmissions. Therefore, this work was motivated to examine the security vulnerabilities and threats imposed by the inherent open nature of wireless communications and to devise efficient defence mechanisms for improving the wireless network security [11]. The security requirements of wireless networks, including their authenticity, confidentiality, integrity, and availability issues were summarized. Next, a comprehensive overview of security attacks encountered in wireless networks is presented in view of the network protocol architecture, where the potential

security threats are discussed at each protocol layer. Similarly, a survey of the existing security protocols and algorithms that are adopted in the existing wireless network standards, such as the Bluetooth, Wi-Fi, WiMAX, and the long-term evolution (LTE) systems were proposed [12].

This letter considers wireless-powered cooperative jamming to secure communication between a transmitter (Tx) and an information receiver, in the presence of an energy receiver (ER), which is termed a potential eavesdropper. The full-duplex jammer harvests energy from the Tx's information signal and transmits jamming signal at the same time, where the jamming signal not only confounds the ER (potential eavesdropper) but also charges the ER. This technique maximizes the secrecy information rate by jointly optimizing the power allocation at the Tx and jammer, while maintaining the harvested energy requirement of the ER. The studied problem is non-convex and the proposed optimal solution based on the Lagrange method. Simulation results show that the proposed scheme significantly outperforms the benchmark schemes [13].

Data integrity attacks (DIA) attempt to insert or alter data to mislead the victim systems to make wrong decisions. To mitigate the vulnerability, model-based and data-driven methods have been proposed. However, model-based methods that rely on the accurate mathematical models of the healthy systems are hard to be used in real applications because of an unavoidable model-reality mismatch for the complexity of power electronics-based smart grids. A new physical layer security scheme in HetNets is designed, where jammer selection along with full-duplex users' artificial noise are used [14]. Significant improvements of the system performance are obtained. Using the tools of stochastic geometry, we derive the expressions of connection probability and secrecy probability. In particular, the locations of active jammers are modelled by a modified Poisson hole process (PHP). Determining the jammer selection threshold is further investigated for connection probability maximization subject to the security constraints. A greedy algorithm is proposed to efficiently solve this problem. The accuracy of the theoretical analysis and the efficiency of the proposed algorithm are evaluated by numerical simulations [15].

Limitations of an existing works:

- Data integrity attacks (DIA) attempt to insert or alter data to mislead the victim systems to make wrong decisions.
- To mitigate the vulnerability, model-based and data-driven methods have been proposed.

- However, model-based methods that rely on the accurate mathematical models of the healthy systems are hard to be used in real applications because of an unavoidable model-reality mismatch for the complexity of power electronics-based smart grids.

Problem Statement:

Different from attack detection where only normal and abnormal data are labeled, attack diagnosis requires more detailed data analysis. Because of the data unbalance that normal condition has a large amount of available data while each attack scenario only has limited available data, accuracies of all data-driven models.

Objective:

- Photovoltaic (PV) systems are becoming more vulnerable to cyber threats.
- Developing cyber-secure power electronics converters has received increased attention from the IEEE power electronics society (PELS) that recently launched a cyber-physical-security initiative.
- The multilayer long short-term memory networks (MLSTM) are used to leverage time-series electric waveform data from current and voltage sensors in PV systems.
- Comparison results verify performances of the proposed method for detection and diagnosis of various data integrity attacks on PV systems.

III. Proposed Work

The proposed cyber security mechanism by combining a one-class detection model and an attack diagnosis model, which are tailored for electric waveform profiles of a solar PV smart grid for real-time attack detection and identification. The one class detection model to detect whether a PV farm is under attack or not. The proposed mechanism has been evaluated using a MATLAB Simulink solar farm model, and achieves much improved attack detection and diagnosis performances. The major advantages of the proposed technique are lower energy consumption and high throughput. Figure 1. Shows the system architecture of the proposed work.

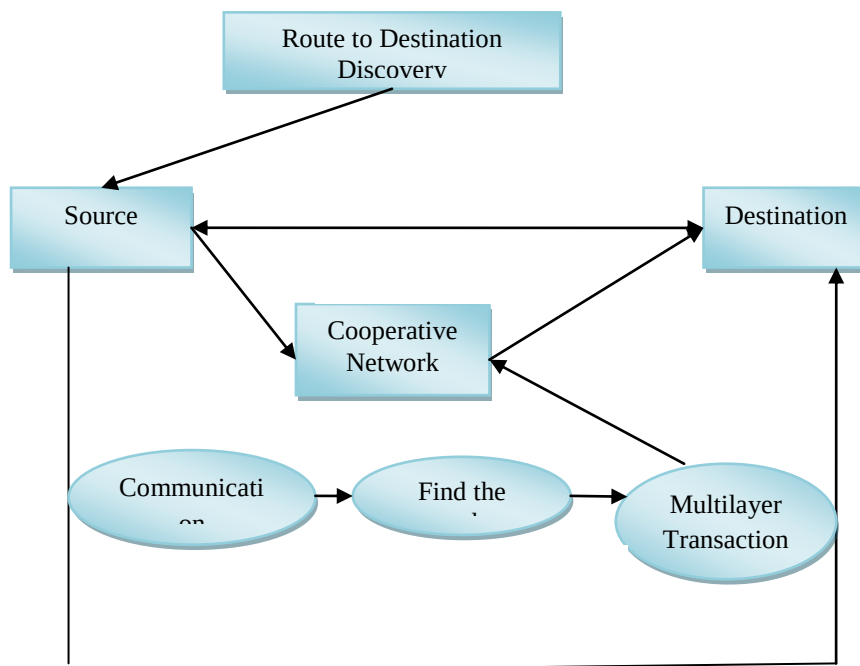


Figure 1. System Architecture

The working principle is discussed as follows:

1. The source node receive the request is in the form of route to destination discovery.
2. Similarly, the destination node sends a path to source node.
3. Now, the source node sends a message to cooperative network (smart grid) and destination node with a jamming free or attack free path.
4. Concurrently, the cooperative network receives a message from the multilayer transmission also.
5. Based on source and multilayer transmission message the cooperative network finds the exact path for the specific data without any attack.
6. If any attack finds a specific route, an alternate path is find based on existing path history.

In the proposed work, the jammer is energy-constrained, e.g., it is battery-powered; hence, its choice of y (i.e., the average duration of the signal emission that jams the packet transmission) stems from a trade-off between two requirements, i.e., i) reduce the amount of information that the target node T can transmit to the perspective receiver, and ii) keep the energy consumption as low as possible. Observe that requirement i) would result in the selection of a high value for y , whereas requirement ii) would result in a low value for y . On the other hand, the target node has to properly choose the value of x (i.e., the maximum

silence period duration scheduled following the transmission of the j^{th} packet and the subsequent jamming signal) in order to maximize the achievable capacity $C(x, y)$, i.e., the amount of information that can be sent by means of the timing channel, while minimizing its energy consumption. Therefore, it is reasonable to consider that the values of x and y represent the strategies for the target node T and the jammer J , respectively. Accordingly, the set of strategies for both players, ST and SJ , can be defined as the set of all the feasible strategies x and y respectively. The following points discussed the working principles of the proposed technique [16].

- **Problem Formulation:** The smart grid measurement at a certain time point is influenced by the states of its previous time points. The electric waveform is recorded for every time interval.
- **Attack Detection Model:** There are various states of PV systems, including the normal state and under-attack states with various attack types. Because it is difficult to accurately detect and identify various types of attacks simultaneously, propose to first focus on detecting whether the PV system is under attack or not. Apply the one-class detection as the attack detection model, which has been widely applied for outlier detection to accurately classify the normal and under-attack states.
- **Attack Diagnosis Model:** The attack identification is actually a classification model based on a multi-classification model to identify attack types. Nevertheless, the seriousness of the same type of attack is also important, but has not been well explored. In addition, the cross-entropy loss function often in practice means a cross-entropy loss function for classification problems and a mean squared error loss function for regression problems.
- **Multilayer LSTM based Deep Sequence Learning:** Since we try to model electric waveform data which have complicated non-linear temporal characteristics, we leverage the LSTM model. The structure of recurrent neural network (RNN) utilizes the information memory at the previous time to apply to the current sequence data prediction.

IV. Experimental results

The smart grid detection and diagnosis of data integrity attacks in solar farms is implemented through MATLAB and java. Two layers are created like smart grid network and multilayer network. Figure 2. Shows the smart grid and multilayer representation.

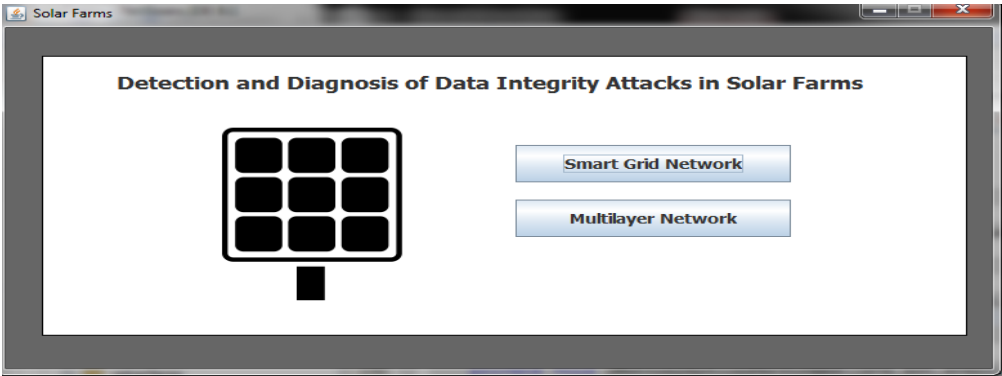


Figure 2. Smart Grid and Multilayer Network Formation

Afterwards, the ID of the node is generated for find the bath between the network. Figure 3. Shows the ID generation of the node by using a detection and diagnosis of data integrity attacks in solar farms based on multi-layer long short term memory network.

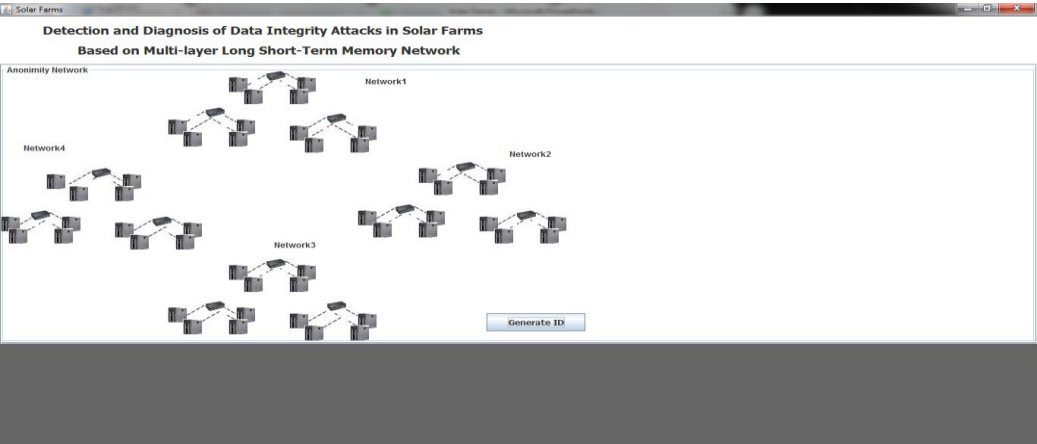


Figure 3. ID Generation

Based on generated ID, the IP address is assigned to each node along with the network details. Figure 4 shows the address generation process. Here the source node along with maximum nodes and destination node distance is given an input.

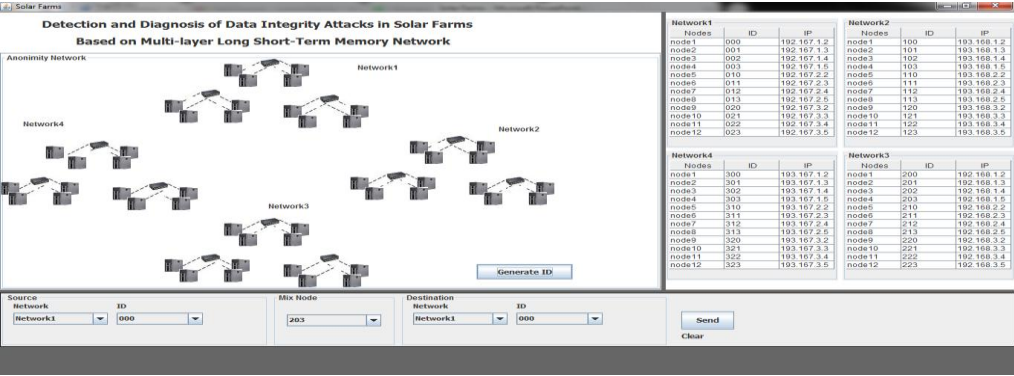


Figure 4. Address Generation

Now, the path between the network and nodes are identified without any attacks. If any attack is identified in between the path, an alternate path will be chosen and transmit the data. Here the data integrity is achieved without compromising the confidentiality. Figure 5 and 6. Shows the Path selection process between the different network nodes.

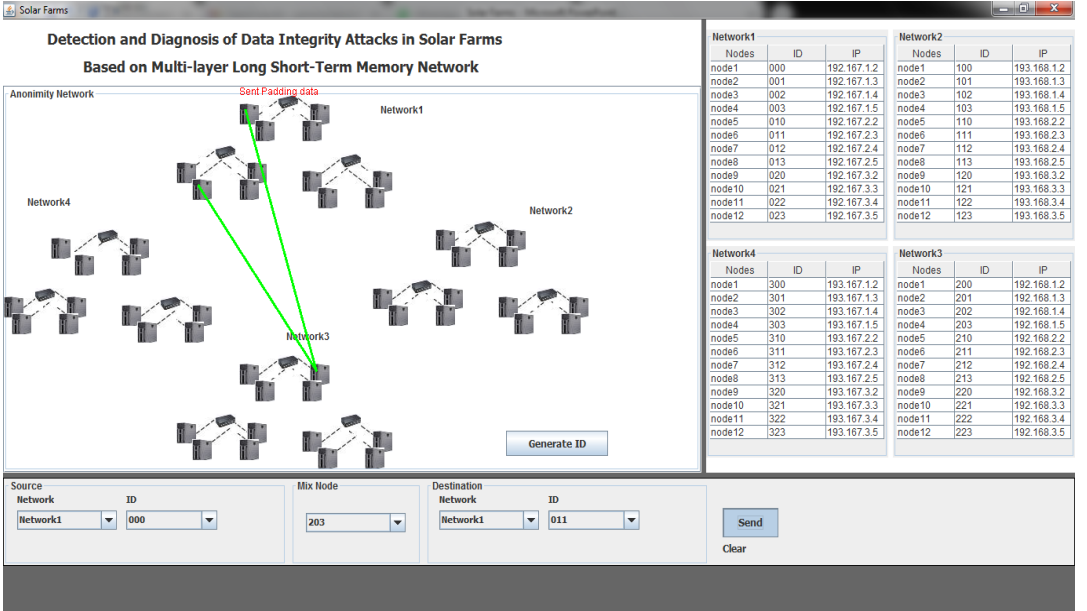


Figure 5. Path selection between network nodes

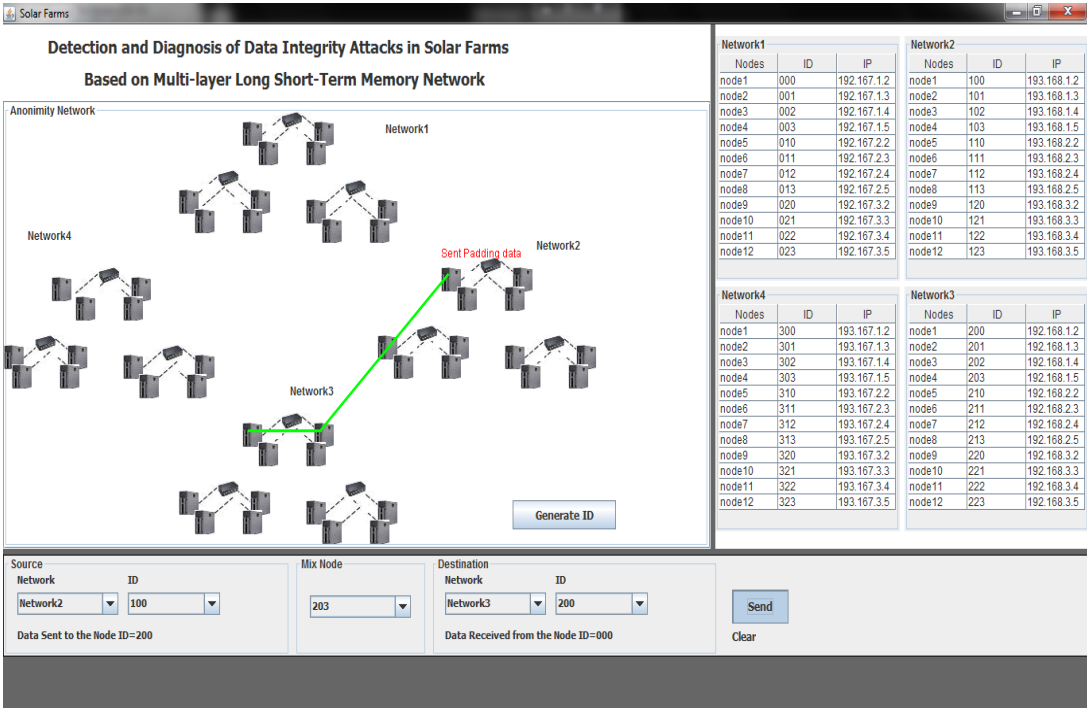


Figure 6. Path selection between network nodes

V. Conclusion

The proposed cyber security mechanism is combined with a one-class detection model and an attack diagnosis model, which are tailored for electric waveform profiles of a solar PV smart grid for real-time attack detection and identification. First, an analysis was conducted on DIA on the smart grid with solar PV farm embedded. Then, an MLSTM based comprehensive approach. The one-class detection model to detect whether a PV farm is under attack or not. When it is detected to be under attack, identify the attack type by leveraging the attack diagnosis model. In future work MLSTM shows a smoother loss curve, which means it potentially has better model robustness and stable performances. Notice that MLSTM demonstrates the best performances when the analysis window size is 80 or 100. Although the metrics achieved another peaks with window size 200, that would be clearly overfitting on interferences.

References

1. W. Tang, S. Feng, Y. Ding, and Y. Liu, "Jammer selection in heterogeneous networks with full-duplex users," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2016, pp. 1–6.
2. A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
3. M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," IEEE Trans. Wireless Commun., vol. 15, no. 4, pp. 3085–3096, Apr. 2016.
4. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," Proc. IEEE, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
5. M. Liu and Y. Liu, "Power allocation for secure SWIPT systems with wireless-powered cooperative jamming," IEEE Commun. Lett., vol. 21, no. 6, pp. 1353–1356, Jun. 2017.
6. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE Trans. Signal Process., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
7. L. Zhang, H. Zhang, D. Wu, and D. Yuan, "Improving physical layer security for MISO systems via using artificial noise," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2015, pp. 1–6.

8. J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multihop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 753–764, Feb. 2016.
9. C. Wang and H.-M. Wang, "Opportunistic jamming for enhancing security: Stochastic geometry modeling and analysis," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10213–10217, Dec. 2016.
10. W. Liu, Z. Ding, T. Ratnarajah, and J. Xue, "On ergodic secrecy capacity of random wireless networks with protected zones," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6146–6158, Aug. 2016.
11. M.Sumathi, R.Lekaa, R.Kavirakshana, N.Nishanthini, K.Nirmala, "Improved CiphertextAttribute Based Sensitive document protection and Secure sharing in cloud storage", *International Journal of Advanced Science and Technology*, Vol. 29, No.03, PP 8702-8708, 2020.
12. M.Rajkamal, M.Sumathi, N.Vijayaraj, S.Prabu, G.Uganya, "Sensitive Data Identification and Protection in a structured and Unstructured data in Cloud Based Storage", *Annals of RSCB*, Vol. 25, Issue.2, 2021, PP 1157-1166.
13. M.Sumathi, M.AafrenFathima, E.Aarthi, S.K.Aarthy and M.Meenakshi, "Resource Scheduling for an Organization Using Round Robin Technique", *International Journal of Advanced Science and Technology*, 2020.
14. M.Sumathi, U.Rahamathunnisa, A.Anitha, Druheen Das, Nallakaruppan. M. K, Comparison of Particle Swarm Optimization and Simulated Annealing Applied to Travelling Salesman Problem, *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 2019.
15. M.Sumathi, S.Prabu, Random Forest Based Classification of User data and Access Protection, *International Journal of Recent Technology and Engineering*, 2019.
16. Sumathi M, Rajkamal M, B.Gomathy, I.Infant raj, SushmaJaiswathi, Swathi D, "Secure Blockchain Based Data Storage and Integrity Auditing in Cloud", *Turkish Journal of Computer and Mathematics Education*, Vol 12, No.9, 2021.