**IDENTIFYING FALSE INJECTION PACKET TRANSMISSION USING SVM AND SECURE OLSR IN WIRELESS SENSOR NETWORKS**

**Abstract**

Wireless Sensor Networks (WSN) is a system of wirelessly communicating, geographically scattered sensor nodes that collect, process, and transmit data. Examples of applications for these networks are smart cities, industrial automation, healthcare, military monitoring, and environmental monitoring. Several research studies have been conducted on securing WSN against false injection attacks, anomaly detection, and optimizing routing protocols. However, most existing approaches face limitations in accuracy, energy efficiency, or security robustness. To resolve the issue, this paper proposes an integrated security framework that combines Support Vector Machines (SVMs) for anomaly detection and Optimal Link-State Routing (OLSR) to achieve secure and efficient routing in a dense WSN environment. Before detecting the anomaly, a Fuzzy clustering method is used to create the cluster and also select the appropriate cluster. After selecting the suitable cluster, the SVM model is trained to detect spuriously injected packets and anomaly nodes. Simultaneously, OLSR ensures secure and energy-efficient routing through cryptographic authentication and trusted path selection. Model outcomes demonstrate that the suggested method accomplishes a Packet Delivery Rate (PDR) of 92% and an accuracy of 95% in detecting false injection attempts. In addition, energy consumption is reduced by 14% compared to traditional routing methods, significantly extending the network lifetime. The results show that integrating SVM and OLSR can effectively suppress false packet injection and improve WSN performance.

**Keywords:** WSN, false injection attacks, fuzzy clustering algorithm, SVM, OLSR, network security.

**1. Introduction**

WSNs are networks of wirelessly connecting, geographically dispersed sensor nodes that gather, process, and send data. WSN are mostly utilized in diverse applications such as industrial automation, military surveillance, and healthcare monitoring. WSNs consist of many sensor nodes that gather data and forward it to a base station [1]. A WSN works by using multiple sensor nodes in a specific area to monitor environmental conditions and transmit the collected data to a central base station. Each node in the network is responsible for sensing the data, processing it, and forwarding it through multi-hop communication using routing protocols. Such packets traverse the network in the best possible way until they reach the base station where they are processed and used in making decisions. [2].

But security vulnerabilities such as spoofing injection packet transmission can affect WSNs. Threshold-based anomaly detection techniques, depending on predetermined rules to define normal and abnormal activity, are incapable of adjusting to dynamic attacks and thus incur a high false positive rate [3]. Trust-based models provide nodes with trust scores based on their actions, but they are prone to collaborative attacks and hence unreliable. [4]. Moreover, traditional clustering algorithms choose cluster heads randomly, leading to poor energy consumption and a higher threat of attacks on key nodes. Because of these shortcomings, an optimized security mechanism is required that can efficiently identify malicious behaviour and preserve network performance. [5].

The SVM model detects real-time anomalies by analysing network traffic properties such as packet size, hop count, transmission rate, and sequence number. Secure OLSR protocol guarantees reliable data transmission by dynamically maintaining routing tables to bypass affected nodes upon detection of a fake injection attack. To effectively detect and neutralise fake injection attacks, this study proposes a hybrid strategy that uses SVM-based anomaly detection, the Fuzzy Clustering Algorithm for cluster head selection, and Secure OLSR routing. Secure OLSR protects against unauthorized access and ensures reliable routing choices by integrating cryptographic authentication and trust-based path choice. This work suggests a hybrid security model which combines three the elements: SVM -based anomaly detection, Secure OLSR routing. The SVM-based anomaly detector tracks network traffic and precisely identifies false injection attacks with minimal false positives. Secure OLSR routing protocol builds on conventional OLSR by including security parameters in route selection to allow data transmission via trusted and uncompromised routes.

**2. Literature Survey**

WSN is an essential technology in contemporary communication systems. It facilitates data gathering and transmission in different applications by placing numerous sensor nodes within a specific region to sense environmental conditions and send the gathered data to a central base station. However, WSNs are susceptible to security flaws including spoofing injection packet transfer. This novel suggests the idea of a fake data injection attack (FDIA). However, according to technical definitions, an FDIA is a system in which knowledge of the functions and characteristics of each component piece is insufficient to comprehend the system's behaviour as a whole completely. [6]

Yet, the security of the Cyber-physical systems (CPS) is compromised by FDI attacks at one or more locations. The CPS is designed using a discrete linear time-constant system with Gaussian white noise. The system has a chi-square detector to detect attacks and a Kalman filter to estimate the state. Rather than analysing attacks at a specific location, it is necessary to analyse the behaviour of the system in the presence of FDI attacks. [7] Due to the limitation of attack resources, in an FID attack, the selection of which sensor is attacked is also given to increase the impact on the system performance. Simulation data is finally presented to validate the theoretical method. Due to the limited attack resources, it only damages the measurement residuals of partial sensors. [8].

They present a false data detection method that uses a fuzzy system. Because they do not need en-route authentication or complex report generation, more energy can be conserved compared to en-route filtering techniques. But most of them generate nodes that entail higher communication and processing overhead during the report generation and forwarding processes, which can result in higher energy consumption [9] These algorithms were either model-based or data-driven. The introduction of the many cyber-attacks and the key historical events is the initial portion of the research. The principal reported incidents in history. The significance and impact of spurious data injection attacks, which can result in higher energy consumption, are then explained. [10].

They suggested to use a sine wave voltage signal with unpredictable Gaussian noise as the Modular Euclidean detector evaluator. Reconfigurable Kalman filters improve the security and monitoring of the intelligent grid system. Detection rate analysis is also performed on attacks like DDOS and random and fake data injection attacks. However, the safe and steady operation of the power system is now significantly influenced by information security. [11] The data integrity attacks are the FDIA which targets the Cyber Physical Power System (CPPS). This approach uses offline training, and the results show the high accuracy and stability, which ensures the steady operation of the smart grid and improves the CPPS's resilience against FDIA However, the safe and steady operation of the power system is now significantly influenced by information security [12].

This fact-based established method is only fact-based. This addresses the limitations of the proposed detection methods and renders the strong to the nonlinear properties and uncertainties of the distribution systems. Various test case scenarios involving a large number of basic and stealth FDIAs are employed to assess the power of the established identifying method. However, these FDIA are so difficult to identify in practice, they pose a difficult challenge to distribution networks [13]. Numerous sensitive data-consuming monitoring, checking, and surveillance systems have employed WSN. The Cluster Head passes further information to the sink node. The experimental results demonstrate that the Blowfish algorithm consumes less energy than the other private key cryptography approaches.

Nevertheless, the encrypted data is vulnerable to errors and can be unlawfully accessed by hackers [14] The enhance the reliability of WSN, in this work they explain the use of network coding techniques combined with appropriate retransmission mechanisms. Essentially, they compare four different retransmission strategies with three applying network coding algorithms combined with the recently discovered Optimised Relay Selection Technique (ORST). The general assumption of this research shows that the ORST combined with network coding will make the communication of WNS more dependable [15].

This work proposes an Extended Kalman Filter Algorithm (EKFA) to detect erroneous inject data in WSN. The shortest path, known as the Path Optimisation Method (POM), is employed in the WSN to identify the obstacle. The EKFA technique improves aberrant node detection and reduces the false negative ratio, according to simulation data. Sensor nodes that are physically dispersed and cooperate with one another make up WSN [16]. The transmit data securely to make a high security root in order to transfer the over industrial network. Routing security problem In Wireless Mesh Networks (WMN) has been widely studied. Numerous solutions exist to solve this issue, but they are different and do not succeed in enhancing WMN security performance.

The technique enhances WMN's security performance and quality of service [17]. Cyclic Analysis Method (CAM)-based intrusion detection algorithm with a combination of forward selection and backward exclusion strategy. Parameters such as network traffic, packet loss, connection, and malicious node detection accuracy are utilized to assess the performance of CAM [18]. The Sensor nodes' resource management, data storage, communication, and computation capabilities are limited.

The wireless sensor nodes could lose their power to communicate with the base station and become dead as a result of network separation segmentation problems [19]. This model applied the Synthetic Minority Oversampling Technique (SMOTE) to tackle the imbalanced dataset issue and Mutual Information (MI) for selecting features. These disadvantages include the inability to identify the right dataset, the issue of feature selection, the imbalanced dataset problem, and the difficulty in selecting the right algorithms for the WSN classification process [20].

**3. Proposed Methodology**

The SVM is used for anomaly detection, while OLSR is enhanced with security mechanisms to prevent false injection packet attacks in WSN. The integration of these two techniques ensures a secure, efficient, and adaptive network communication process. This methodology ensures a robust and secure WSN capable of detecting and mitigating false injection attacks while optimizing network performance.

Cluster Head

Sensor nodes

Cluster Location

Fuzzy Clustering

Secure OLSR Routing

Secure Transmission

Secure OLSR Routing

**Figure 1: Architecture Diagram for Proposed SVM and** **OLSR Method**

The above architecture diagram depicts the data flow in WSN, which incorporates SVM-based false injection detection and SOLSR to provide secure and effective data transmission as shown in figure 1. Sensor nodes exchange information with their individual cluster heads, which then efficiently control data transmission. Clustering offers improved scalability, less poor consumption, and better overall wireless sensor network performance. The WSN is divided into several clusters, and the CH is selected by a fuzzy clustering algorithm. The CH is responsible for efficiently forwarding and aggregating data from sensor nodes, enhancing network stability and reducing energy usage. To counter FDI attacks, the sensor nodes' collected data is filtered through an SVM-based detection mechanism. SVM identifies the incoming packets as legitimate or malicious, depending on specific features extracted from the network traffic. When an anomaly is found, the malicious packets are dropped to ensure they do not influence the network. After genuine data packets are recognized, they are forwarded via the Secure OLSR protocol. By selecting the most effective packet-forwarding routes and including security measures to thwart threats like routing misdirection and node intrusion, OLSR increases routing efficiency. Following secure routing, data integrity, dependability, and decreased latency are guaranteed as the authorized data is securely sent to its intended location. By strengthening their defences against bogus injection assaults and preserving their high data transfer performance, this procedure improves the general security and effectiveness of WSNs. This architecture enhances the resilience and reliability of WSNs in safety-related applications by combining trusted routing protocols with anomaly detection through machine learning.

**3.1 Fuzzy Clustering Algorithm**

In WSN, Fuzzy Clustering Algorithm is critical in optimizing the CH selection. This method improves network lifetime, load balancing, and energy conservation. The best cluster heads are chosen and sensor nodes are dynamically created using the fuzzy algorithm. In contrast to conventional clustering techniques, FCA gives nodes membership values, enabling more flexible cluster formation according to network circumstances. This improves safe interactions between clusters and lowers energy use.

Each sensor node is assigned a membership function based on critical parameter. The proximity of the node to the base station. A fuzzy logic system is applied to compute the CH membership value for each node. Each node calculates its Cluster Head Probability (CHP) using the equation

In the process of selecting an optimal Cluster Head (CH) in a Wireless Sensor Network (WSN), multiple factors must be considered to ensure efficient energy utilization and network longevity. The Cluster Head Priority of a node iii is determined using a weighted function that takes into account three key parameters: residual energy , node density , and the distance to the Base Station . Let assume are weight coefficients (typically sum to 1), are normalized fuzzy functions mapping values between [0,1], The priority function is expressed as equation 1.

(1)

Nodes with higher CHP values are more likely to become cluster heads. Nodes with the highest CHP values within a local competition radius become CH. The final cluster head selection is performed using. To efficiently select a CH in a Wireless Sensor Network (WSN), a threshold-based decision mechanism is employed. The Cluster Head status of a node iii is determined based on its CH Priority . where ​ is a predefined threshold value based on network conditions. The selection criterion is defined as equation 2.

(2)

**3.2 Support Vector Machines** (**SVM)**

SVM is the performs classification and regression. It operates by determining an optimal hyperplane that can best segregate data points into various classes in an N-dimensional space. In anomaly detection within WSNs, SVM can be utilized to differentiate between normal and malicious packet transmission through the examination of network factors such as packet rate of arrival, transmission delay, and node activity. Since the project does not rely on a predefined dataset, the security node continuously monitors network traffic and extracts key parameters from real-time packets, including: Packet Size – Abnormal packet sizes may indicate malicious data, Hop Count – Unexpected hop counts suggest a compromised path, Transmission Rate – Nodes injecting false packets typically send at an irregular rate, Sequence Number – Irregular packet sequences could indicate an attack. These extracted features serve as input data for the SVM-based anomaly detection system.

Initially, the security node observes normal network behaviour and creates a baseline. When anomalies are detected, the SVM model dynamically learns and refines the classification ability. The SVM classifier is trained with Normal Packets → Label , Malicious Packets → Label , The Linear Kernel SVM is chosen for fast and efficient classification. Equation for SVM Decision Boundary SVM is a supervised machine learning algorithm that finds the best decision boundary to separate normal and malicious packets. = Feature vector extracted from network packets , = Weight vector that determines the decision boundary, = Bias term to shift the decision boundary, = Classification function. The classification function in SVM is represented as equation 3:

(3)

The decision rule for classification is the packet is classified as normal, , the packet is classified as malicious (false injection attack). Support Vector Classification Process: Feature Extraction: The security node extracts feature from network packets such as: Packet size , Hop count , Transmission rate , Sequence number in equation 4.

(4)

Optimal Hyperplane Calculation: The weight vector, w, specifies the direction of the decision boundary. The feature vector, is a point in input space. The dot product of the weight vector and the feature vector is . The bias term that moves the decision border is bbb. This equation represents a hyperplane that classifies distinct classes in an n-dimensional space. This hyperplane is utilized to classify points in SVM. The optimal hyperplane that separates normal and malicious packets is determined using the equation 5.

(5)

The margin between support vectors is maximized by minimizing the objective function: The feature vector contains information such as packet transmission behaviour, node energy levels, and routing anomalies. The SVM classifier finds an optimal decision boundary to distinguish between legitimate packets and false injection attacks. By minimizing , the system achieves a clear separation between normal and attack behaviours, improving detection accuracy and reducing false positives. equation 6.

(6)

subject to the constraints: ​ is the true class label of the th data point, where . is the feature vector representing the th data point. is the weight vector, defining the orientation of the decision boundary. is the bias term, shifting the decision boundary. is the decision function that determines on which side of the hyperplane lies. The margin is the distance between the two parallel hyperplanes at and , ensuring maximum separation between the two classes in equation 7.

(7)

where is the actual label of the packet When a new packet arrives, SVM evaluates the feature vector using the decision function in equation 8.

(8)

, the packet is forwarded. , the packet is discarded. The decision boundary, given by separates the two classes. The SVM maximizes the margin between the closest data points and the decision boundary, improving classification accuracy.

**3.3 Optimized Link State Routing (OLSR)**

This section discussed the OLSR method as a secure and efficient routing in the WSN environment. A proactive routing protocol named OLSR is developed for WSN and mobile ad hoc networks. To prevent fake injection attacks and provide secure and efficient routing, the OLSR is used. and OLSR is updated to avoid routing through the malicious node. OLSR is a proactive routing protocol, meaning continuously updates routing tables even before data transmission begins. Each sensor node maintains updated information about the entire network topology. The protocol selects Multi-Point Relays (MPRs), which reduce the number of transmissions needed, improving network efficiency. OLSR is a proactive routing protocol where each node maintains an updated routing table. Secure OLSR enhances this by incorporating trust-based path selection and cryptographic authentication.

The standard OLSR protocol selects the best route by minimizing the total hop count in equation 9.

(9)

= Total distance between source and destination . ​ = Hop count for the th link. The path with the minimum is selected. Instead of selecting paths based on hop count alone, Secure OLSR integrates a trust factor for each node, ensuring that paths with higher security are prioritized. = Trust score of nodes , calculated based on previous packet forwarding behaviour. Malicious nodes have low trust values, increasing , and are avoided in routing decisions. To prevent unauthorized packet injections, each routing message is digitally signed using hash-based authentication. The modified routing metric is equation 10.

(10)

(11)

The equation 11, = Cryptographic hash of the message, = Routing packet, = Secret key shared between nodes. If a received packet’s hash does not match the expected value, is identified as a false injection attack and discarded. Each node can compute and verify incoming packets using the expected hash value. The network's security will be enhanced if an attacker tries to insert a malicious packet since the disparity in hash values will cause anomaly detection.

**4. Results and Discussion**

The experimental results compare the AODV and FID methods with this OLSR Method. The optimized and secure route is established, ensuring high Packet Delivery Ratio (PDR). SVM ensures accurate anomaly detection, preventing false injection attacks. Secure OLSR ensures resilient routing, preventing malicious nodes from disrupting communication. Nodes select trusted MPRs to relay packets efficiently. If an anomaly is detected, OLSR updates the routing table to avoid compromised nodes. The proposed system evaluated the through simulations in a WSN environment consisting of 100 randomly deployed sensor nodes. The network is tested under both normal conditions and false injection attack scenarios to measure the impact of the SVM-based anomaly detection and Secure OLSR routing. The key performance metrics analysed include Detection Accuracy, PDR, and Energy Consumption.

**Table 1. Simulation Setup**

|  |  |
| --- | --- |
| Platform | NS-2 simulator |
| Network Topology | 100 sensor nodes. |
| Traffic Model | CBR |
| Attack Model | FDI |

The table 1 shows the simulation configuration employed to test the suggested method. NS-2 simulator is selected as the simulation tool because of effectiveness in simulating WSN. The network topology includes 100 sensor nodes to provide a realistic field deployment. CBR traffic model is employed, which provides a fixed packet transmission rate, and thus the ideal for testing network performance. The attack scheme uses FDI, where attacking nodes inject forged packets into the network such that one can test the system's capability to detect and remedy the same.

**Figure 2: Throughput Performance Analysis**

Figure 2 is used to compare the throughput performance of AODV is 700kps, OLSR, and FID. The x-axis is throughput in kbps and the y-axis is various scenarios or time. OLSR: Shows the greatest throughput in all cases, reaching more than 900 kbps in the ideal case. OLSR keeps proactive routing tables, so packets are forwarded fast and securely. AODV: Obtains moderate throughput but is less than OLSR. AODV is a reactive protocol that adds route discovery delays, lowering throughput performance. FID: Indicates better throughput than AODV but is marginally less than OLSR. The proposed Secure OLSR with SVM-based anomaly detection increases packet transmission by avoiding false injections but adds marginal cryptographic processing overhead.

**Figure 3: Performance Latency Analysis**

Figure 3 performance latency analysis compares the packet transmission delay for three routing protocols: AODV, OLSR, and FID. The latency increases with the number of nodes in all protocols because more network congestion and processing overhead are involved. AODV has the 95ms most excellent latency as the takes a reactive routing method and waits for route discovery prior to sending, a process that prolongs packet sending time significantly, especially as network scale increases. OLSR is 30ms at the opposite end with minimal latency as its proactive routing implies precomputed routing tables that can quickly forward packets. The proposed Secure OLSR presents a minor additional latency over conventional OLSV because of the additional processing for SVM-based anomaly detection and cryptographic authentication. However, has considerably less latency than AODV while ensuring packet transmission that is secure and efficient. The findings confirm that although Secure OLSR compromises a bit on latency in Favor of increased security, the still highly efficient and more delay-effective compared to AODV and, therefore, an appropriate candidate for secure WSN applications.

**Figure 4: Energy Efficiency Analysis**

Figure 4 protocols AODV, OLSR, and proposed Secure OLSR are analysed for energy efficiency in the current analysis. AODV is 7.52% energy-intensive with frequent route discoveries and retransmissions resulting from false injection attacks, which wastes resources. OLSR is 15.6% more energy-efficient because they support proactive routing tables that minimize routing overhead. Nevertheless, they have no security provisions. The Secure OLSR proposed enhances energy efficiency through reduced retransmissions due to FDI, secure path optimization, and less wastage of energy. Although the additional security measures impose minor computational overhead, the overall efficiency is still greater than AODV, thus a balanced solution for secure and energy-efficient WSN applications.

**Figure 5: Energy Use Analysis**

As shown in Figure 5, the energy consumption graph displays the power usage of several routing protocols, including OLSR, AODV, and the recently introduced Secure OLSR. When there are a lot of nodes, AODV uses 9.2% the most energy. The reason for this is that is a reactive protocol that incurs additional energy overhead due to frequent route discoveries and retransmissions. However, because OLSR actively updates routing tables and restricts the number of routes that can be found, they use less energy is 5.2%. However, typical OLSR has no built-in security safeguards, which could lead to erroneous data insertion, excessive transmissions, and energy waste. The OLSR proposed here attains energy-optimized use by combining anomaly detection and cryptographic authentication to assist in retransmission minimization due to false injection attacks. While security protocols add minimal computational overhead, overall energy consumption is less than AODV but still has good security. The results verify that FID maintains an effective balance between security and energy consumption and, hence, is a more efficient option for WSN applications where energy conservation is essential.

**Figure 6: Packet Loss Performance Analysis**

As shown in Figure 6 the number of packets transmitted; PDR determines the data transmission efficiency of a WSN. Higher network resistance to packet loss is reflected in an increased PDR. As per the graph, OLSR achieves the maximum PDR of any node density, with approximately 90% at 400 nodes specifically. This is due to its proactive routing mechanism, which maintains routing tables current and ensures efficient packet delivery. While AODV operates fairly well, PDR enhancement decelerates as the number of nodes increases. This is due to its reactive nature, which causes delays and potential packet loss because of repeated route discovery. Since security methods such as SVM-based anomaly detection and cryptographic authentication introduce computing complexity, FID has a consistent PDR but operates slightly less efficiently than OLSR. They still outperform AODV, however, in showing its capacity to maintain packet communication secure and efficient.

**Figure 7: Packet Loss Performance Analysis**

Figure 7 described a Packet loss refers to network inefficiencies when data packets are not delivered to their destinations. AODV suffers 30% from the highest packet loss, particularly at low node densities, caused by high-frequency route discoveries. OLSR registers the least packet loss through proactive routing and effective data transfer is 8%. FID (Secure OLSR Proposal) sustains modest packet loss, lower than AODV but higher than OLSR due to SVM-based anomaly detection security overhead and cryptographic authentication. OLSR, on the whole, reduces packet loss efficiently, whereas FID provides a secure and reliable equilibrium for WSN applications.

**Figure 8: Network Lifetime Analysis**

Figure 8 shows OLSR gets the maximum network lifetime, followed by OLSR and AODV. AODV gets the minimum lifetime as there are a lot of route discoveries and more energy usage. OLSR gets better performance compared to AODV 1300s due to proactive routing, which decreases route request overhead. OLSR gets a considerable increase in network lifetime by adding energy-efficient routing and security features, stopping FDI attacks that lead to useless retransmissions. Therefore, OLSR provides a more stable and reliable WSN deployment.

**5. Conclusion**

This paper proposed an efficient security framework for WSN to mitigate false injection packet attacks using a combination of an SVM for anomaly detection, Secure OLSR for routing, and a Fuzzy Clustering Algorithm for optimal cluster head selection. The proposed method effectively detects malicious nodes, ensuring secure data transmission while optimizing energy efficiency. The integration of SVM enhances attack detection accuracy, Secure OLSR improves routing reliability, and fuzzy clustering prolongs network lifetime by balancing energy consumption. Simulation results demonstrate high detection accuracy (85%), low false positive rate (5%), and a significant improvement in packet delivery ratio (90%) under attack conditions. The proposed method offers superior robustness against adversarial threats compared to traditional security mechanisms. Future work will focus on deep learning techniques for advanced anomaly detection and lightweight cryptographic mechanisms to enhance real-time security in resource-constrained WSN environments.

**Reference**

1. S. Ghosh, M. R. Bhatnagar, W. Saad and B. K. Panigrahi, "Defending False Data Injection on State Estimation Over Fading Wireless Channels," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1424-1439, 2021.
2. L. C. Mutalemwa and S. Shin, "Comprehensive Performance Analysis of Privacy Protection Protocols Utilizing Fake Packet Injection Techniques," in IEEE Access, vol. 8, pp. 76935-76950, 2020, doi: 10.1109/ACCESS.2020.2989434.
3. Kaushik, Sheetal, et al. "Performance analysis of AODV and SAODV routing protocol using SVM against black hole attack." *2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM)*. Vol. 2. IEEE, 2022.
4. Dutt, Inadyuti, Samarjeet Borah, and Indra Kanta Maitra. "Immune system-based intrusion detection system (IS-IDS): A proposed model." *IEEE Access* 8 (2020): 34929-34941.
5. M. A. Al-Naeem, "Prediction of Re-Occurrences of Spoofed ACK Packets Sent to Deflate a Target Wireless Sensor Network Node by DDOS," in IEEE Access, vol. 9, pp. 87070-87078, 2021, doi: 10.1109/ACCESS.2021.3089683.
6. Ahmed, M., Pathan, AS.K. False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. Complex Adapt Syst Model **8**, 4 (2020).
7. Padhan, Sushree, and Ashok Kumar Turuk. "Design of false data injection attacks in cyber-physical systems." Information Sciences 608 (2022): 825-843.
8. Guo, Haibin, Jian Sun, and Zhong-Hua Pang. "Residual-based false data injection attacks against multi-sensor estimation systems." IEEE/CAA Journal of Automatica Sinica 10.5 (2023): 1181-1191.
9. Lee, Hae Young, Tae Ho Cho, and Hyung-Jong Kim. "Fuzzy-based detection of injected false data in wireless sensor networks." International Conference on Information Security and Assurance. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.
10. Musleh, Ahmed S., Guo Chen, and Zhao Yang Dong. "A survey on the detection algorithms for false data injection attacks in smart grids." IEEE Transactions on Smart Grid 11.3 (2019): 2218-2234.
11. Dayananda, Prakyath, et al. "Efficient detection of faults and false data injection attacks in smart grid using a reconfigurable Kalman filter." International Journal of Power Electronics and Drive Systems (IJPEDS) 13.4 (2022): 2086-2097.
12. Cao, Jie, et al. "A novel false data injection attack detection model of the cyber-physical power system." IEEE access 8 (2020): 95109-95125.
13. Ahmed S. Musleh, Guo Chen, Zhao Yang Dong, Chen Wang, Shiping Chen, Spatio-temporal data-driven detection of false data injection attacks in power distribution systems, International Journal of Electrical Power & Energy Systems,Volume 145,2023,108612,ISSN 0142-0615.
14. Singh, Anuj Kumar, et al. "Secure and Energy Efficient Data Transmission Model for WSN." Intelligent Automation & Soft Computing 27.3 (2021).
15. Laurindo, Suelen, et al. "Combining network coding and retransmission techniques to improve the communication reliability of wireless sensor network." *Information* 12.5 (2021): 184.
16. R. Babuji, J. J. Ganesan, D. Lekha, M. Karthikeyan and D. M. Kalai Selvi, "Extended Kalman Filter Algorithm to Detect False Data Injection in Wireless Sensor Network," 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2023.
17. Sathya, S. S., and K. Umadevi. "RETRACTED ARTICLE: An optimized distributed secure routing protocol using dynamic rate aware classified key for improving network security in wireless sensor network." *Journal of Ambient Intelligence and Humanized Computing* 12.7 (2021): 7165-7171.
18. Visalakshi, P. "Connect attack in -WSN detect through cyclic analysis based on forward and backward elimination." PeerJ Computer Science 10 (2024): e2130.
19. Roberts, Michaelraj Kingston, and Poonkodi Ramasamy. "An improved high-performance clustering-based routing protocol for wireless sensor networks in." *Telecommunication Systems* 82.1 (2023): 45-59.
20. Al-Fuhaidi, Belal, et al. "Anomaly‐Based Intrusion Detection System in Wireless Sensor Networks Using Machine Learning Algorithms." *Applied Computational Intelligence and Soft Computing* 2024.1 (2024): 2625922.