INTELLIGENT TRUST MANAGEMENT AND INTRUSION MITIGATION IN IOT WIRELESS SENSOR NETWORKS USING DEEP LEARNING

Satish Dekka
Research Scholar
Shri JJT University
Rajasthan.

Dr. Prasadu Peddi
Guide
Shri JJT University
Rajasthan.

Dr. Manendra Sai Dasari
Co-Guide
Shri JJT University,
Rajasthan.

ABSTRACT

The Internet of Things (IoT) enables transformative applications; however, it faces significant security and privacy challenges. Due to the impracticality of securing individual devices, network-level security is preferred. However, attack diversity, device heterogeneity, and traditional security limitations necessitate advanced data analysis. Researchers increasingly use deep learning, which excels in handling large-scale data, to develop robust intrusion detection systems. Performance was evaluated using standard classification metrics including accuracy, precision, recall, and F1-score. Intrusion detection in Wireless Sensor Networks (WSNs) is an emerging area of research, given their extensive use in sensitive fields like military surveillance, healthcare, environmental monitoring, and smart cities. Their deployment in open, unattended environments makes them especially vulnerable to threats like eavesdropping, interference, and jamming. To address this problem, Random Forest (RF) is a popular machine learning model. The RF model can be tweaked because of its multiple hyperparameters.

Keywords: *Internet of Things (IoT), Wireless Sensor Networks (WSNs), Random Forest (RF), machine learning model, network-level security.*

INTRODUCTION

With the development of IoT (Internet of Things, IoT), wireless sensor networks have been widely used in environmental monitoring, smart home, industrial production, military and medical fields. The resources of Wireless sensor node are limited especially in terms of computation and energy. Those nodes are often deployed in unmanned and complicated environments. WSNs are vulnerable to the attacks that include node capture, Sybil attack and black-hole etc. More and more researchers study to improve the network performance by effectively resist malicious nodes. Wireless Sensor Networks are generally defined as the dedicated and spatially distributed sensors in groups that are commonly used for the purpose of recording and monitoring the environmental conditions. The measuring capabilities include measurements of pressure, temperature, sound, humidity, pollution levels, wind direction, and speed, etc. Some of the significant applications of WSNs include tracking the target and remote monitoring of the environment. These applications are possible only because of the sensors which are easily accessible, cheaper, intelligent and small. Sensors generally have the capability of communicating with one another to form a network by providing wireless interfaces. Difficulties in WSNS can be classified as stacking of the protocol in the communication servicing, provisioning and using the network and underlying operating system and its internal platforms. Localization of inaccurate rate and target tracking in a wireless sensor network constitute limited and inexpensive accuracy components.

LITERATURE REVIEW

Laila Tageldin et.al. (2025) The Internet of Things (IoT) is regarded as the driving force behind the Fourth Industrial Revolution. The convergence of IoT, cloud computing, and smart environments can help ensure people's well-being. One major problem for IoT networks is protecting privacy and overcoming security threats. This study discusses security threats across IoT networks, which can lead the researchers to develop and implement industry-wide security standards and certifications. In addition, this study emphasizes the importance of data protection and discusses the security measures and mitigation approaches to secure personal and sensitive information, as well as other security threats within such environments. That will assist researchers in developing an efficient, scalable, resilient, and precise intrusion detection system for IoT devices to counter large-scale attacks.

Malliga Subramanian et.al. (2025) This study presents a systematic review of deep learning (DL) techniques for Network-based Intrusion Detection Systems (NIDS) based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses: (PRISMA2020) guidelines. It explores recent advancements in data preparation, DL architectures, and performance evaluation metrics for NIDS. The review provides insights into various datasets and tools used in the field, highlighting the effectiveness of DL in improving NIDS performance. Additionally, it discusses the applications of NIDS across different industries and identifies emerging research trends, offering a comprehensive resource for researchers and practitioners in cybersecurity.

M. Sakthimohan et.al. (2024) In general, wireless sensor networks are used in various industries, including environmental monitoring, military applications, and queue tracking. To support vital applications, it is crucial to ensure effectiveness and security. To prolong the network lifetime, most current works either introduce energy-preserving and dynamic clustering strategies to maintain the optimal energy level or attempt to address intrusion detection to fix attacks. In addition, some strategies use routing algorithms to secure the network from one or two attacks to meet this requirement, but many fewer solutions can withstand multiple types of attacks. So, this study proposes a secure deep learning-based energy-efficient routing (SDLEER) mechanism for WSNs that comes with an intrusion detection system for detecting attacks in the network. The proposed system overcomes the existing solutions' drawbacks by including energy-efficient intrusion detection and prevention mechanisms in a single network.

Deny. J et.al. (2024) In general, wireless sensor networks are used in various industries, including environmental monitoring, military applications, and queue tracking. To support vital applications, it is crucial to ensure effectiveness and security. To prolong the network lifetime, most current works either introduce energy-preserving and dynamic clustering strategies to maintain the optimal energy level or attempt to address intrusion detection to fix attacks. In addition, some strategies use routing algorithms to secure the network from one or two attacks to meet this requirement, but many fewer solutions can withstand multiple types of attacks. So, this study proposes a secure deep learning-based energy-efficient routing (SDLEER)

mechanism for WSNs that comes with an intrusion detection system for detecting attacks in the network.

A. Merline et.al. (2023) In the Wireless Multimedia Sensor Network (WNSMs) have achieved popularity among diverse communities as a result of technological break throughs in sensor and current gadgets. By utilising portable technologies, it achieves solid and significant results in wireless communication, media transfer, and digital transmission. Sensor nodes have been used in agriculture and industry to detect characteristics such as temperature, moisture content, and other environmental conditions in recent decades. WNSMs have also made apps easier to use by giving devices self-governing access to send and process data connected with appro-priate audio and video information.

Wireless Medical Sensor Network

The importance of WMSN and its critical role in healthcare systems motivate the standardization process to enable the interoperability of different products from different vendors. IEEE 802.15.6 defines the Physical (PHY), and the Medium Access Control (MAC) layers. The extremely rigorous requirements of WMSN transceivers, such as power efficiency, force IEEE Task Group 6 (TG6) to adopt three types of physical layers in order to satisfy different types of applications. These physical layers could be summarized as follows:

- **Narrowband (NB) PHY:** supports seven frequency bands with different data rates.
- **Ultra-wideband (UWB) PHY:** supports two different frequency bands, low and high, with a different number of channels while having the same bandwidth. The design of UWB PHY provides durable implementation with lower complexity and power consumption.
- **Human body communication (HBC) PHY:** supports one low-frequency band centered at 21 MHz, where the data transmission is conducted through the patient's body using Electric Field Communication (EFC) technology.

Design Characteristics

The overall design characteristics of the IEEE 802.15.6 standard are as follows:

- Recoverable in case of any link or node failure.
- The ability to support a vast range of data rates starting from tens of Kbps and up to around 10 Mbps in order to meet all potential applications.
- Provides efficient power consumption mechanisms that allow the power source to last for several years.
- Provides reliable communication with acceptable jitter and latency values for both medical and non-medical applications.
- Supports the coexistence of both in-body and on-body sensor nodes.
- Able to support authentication, encryption, and integrity security mechanisms.
- Able to address node adding and removing within a relatively short time.
- Supports operation in a heterogeneous wireless environment.
- Complies with Specific Absorption Rate (SAR) regulations.
- Supports scalability up to 64 nodes.

WMSN Topology

The IEEE 802.15.6 defines the network as a logical set consisting of sensor nodes and a single hub. It adopts the star topology with two different types of communications, simple one-hop and extended two-hop star topology. In simple one-hop star topology, nodes exchange frames directly with the hub. In contrast, in the extended two-hop topology, a relay node is introduced, and nodes are able to communicate directly with the hub or via a relay node. The total number of nodes is specified by the MAC sublayer parameter mMaxBANSize, which has been set to 64. Sensor nodes (SNs) could be classified based on their role into:

- **Hub:** The hub node, the sink node, or the coordinator are different names for the same node type. The hub acts as a gateway to external networks. It controls the WMSN, and all the external communications go through it. It has better resources compared to normal nodes inside the network.
- **Relay node:** Some nodes have the relay capability to relay messages from end nodes to the hub. They are located in the hub's direct communication range.
- **End node:** Other nodes are considered end nodes. They are designed to perform specific tasks and exchange messages with the hub directly if they are in the direct communication range or via relay nodes if they are out of the direct communication range.

Security in WMSN

Security and privacy issues are critical concerns in all types of networks. However, WMSN, which processes critical data that, if compromised, may affect patients' health or endanger their lives, requires more effective security mechanisms to protect patients from all types of malicious activities. Although security in WMSN is crucial and has a high priority, there are still many open areas to research due to its strict resource restrictions, in addition to a wide range of security and privacy vulnerabilities inherited from WSN. In order to ensure a high level of security and privacy, secure and reliable data delivery must be guaranteed. The basic security requirements could be outlined as follows:

- **Confidentiality:** Data must be protected from being disclosed to any unauthorized parties during data transmission as well as during the storage phase. Data in WMSN contains very sensitive information about the health of the patient. It could be disclosed during transmission in an open channel by eavesdropping or could be disclosed when it is stored in a plain format when a node gets compromised.
- **Integrity:** When data is received, the receiver party has to ensure that the received information is original and has not been altered during the transmission phase. Confidentiality measures cannot protect data from modification, which can be easily done by intercepting data in the transmission phase to inject, delete, or modify the sent message.
- **Availability:** Adversary can breach the availability and prevent authorized entities from accessing the required data. Considering the critical applications of WMSN, disrupting the communication between the caregivers and sensor nodes may threaten the patient's

life. Therefore, maintaining the ability to access the required data under any circumstances is a crucial requirement for this kind of applications.

- **Data Authentication:** While data integrity aims to save data from being modified during the transmission, data authentication aims to ensure that the received message came from the origin node, which is believed to be.

IEEE 802.15.6 defines the Message Authentication Code (MAC) to verify that the received message is sent by the original sender.

- **Data Freshness:** Adversary may intend to capture the transmitted messages and replay them afterward, which causes confusion and instability in WMSN. Therefore, a mechanism to ensure that the received message is recent and that no adversary replays old messages is a must. Ensuring that the received messages are in order and on time is referred to as strong freshness, whereas there is no latency guarantee in weak freshness.
- **Secure Management:** Many security mechanisms such as encryption, decryption, and data authentication require keys, which must be distributed in a secure manner.

IEEE 802.15.6 defines three levels of security, where the hub and the sensor nodes can choose from. Each one of these security levels has different security characteristics as follows:

- **Level-0 Unsecured Communication:** No security measures are used at this level of security. Messages are exchanged in unsecured frames without confidentiality, authentication, integrity validation, or replay defense.
- **Level-1 Authentication:** Messages, at this security level, are exchanged in secured authenticated frames that ensure message authenticity, replay defense, and integrity validation. However, no measures are applied to provide confidentiality and privacy protection.
- **Level-2 Authentication and Encryption:** The highest level of security proposed in the standard. Messages are exchanged in secured, authenticated, and encrypted frames. Therefore, confidentiality, message authenticity, integrity, and replay defense are all provided at this security level.

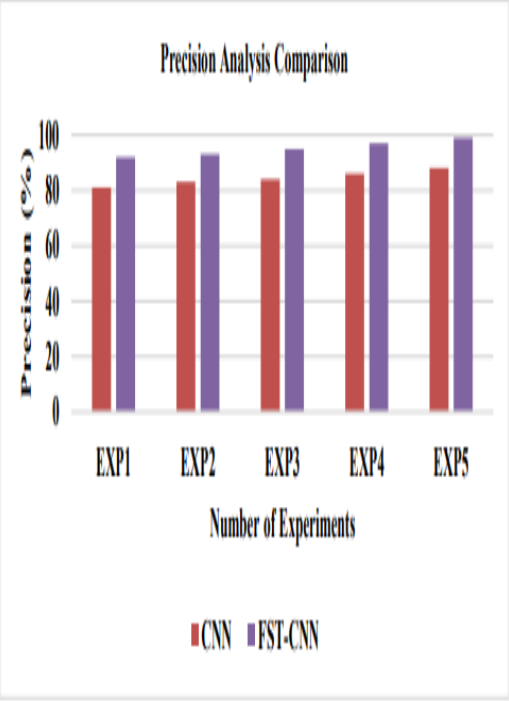
RESEARCH METHODOLOGY

The newly developed IDS based secured routing protocol named Fuzzy Spatial Temporal Convolutional Neural Network based LEACH (FST-CNNLEACH) that detects intrusive behaviours at an early time and routes data securely. This IDS-routing strengthens the communication security in IoT based WSN routing through the selection of paths having only genuine nodes. The member components of this proposed IDS routing system and it contains the components IoT sensor nodes, Network trace-data, Benchmark IDS-dataset, the data gathering module, the Clustering Module (CM), the EM, the constraint-manager, the deep CNN based Spatial Temporal IDS, the FR based DM, LEACH-IDS secure routing module, and

fuzzy-rule base. The data related to node locations are sent directly to the clustering module. Moreover, the data preparation for trace data involves the identification of the spatial constraints and temporal constraints that are needed to clean the network data. In the Benchmark data pre-processing, first the row selection is done by selecting the rows with minimum number of null values that are present in a tuple. In attribute selection, the strength of the attributes with respect to their usefulness in the classifier's convergence is the most important criteria for selecting the attributes.

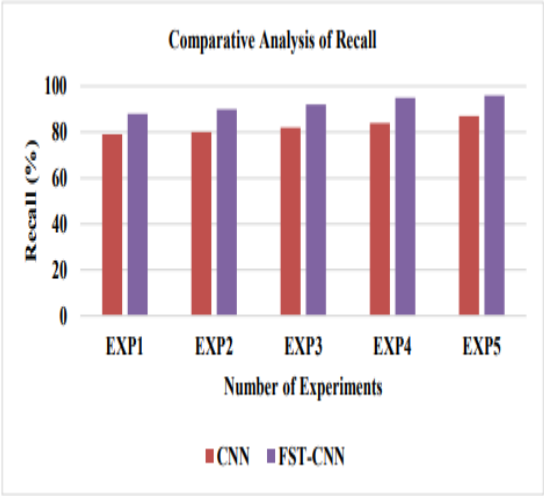
RESULTS AND DISCUSSIONS

Using the experiments on FST-CNN, it is concluded that this FST-CNN detects the intrusive behaviours correctly. This system was implemented using NS-3 and Python with two datasets. The metrics namely Accuarcy_values, Precision_values, Recall_values and F-measure_values are used in this thesis for effective validation of FST-CNN and other related works.



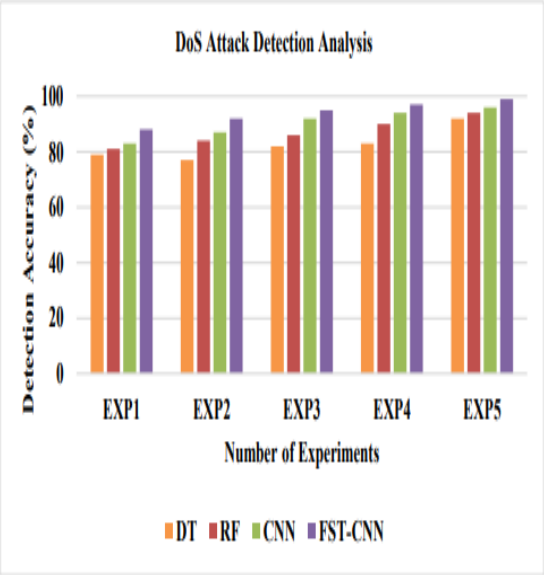
Graph 1: Precision analysis comparison

With Graph. 1, it is proved that the precision value given by FST-CNN is higher than the corresponding values provided by CNN. The use of SE based temporal analysis, FPI based spatial and mobility modelling and fuzzy reasoning in FST-CNN made it to perform better than CNN with respect to precision values. Graph 1 depicts the Recall_values comparision among CNN and FST-CNN. From Graph. 2, it is evident that FST-CNN performs CNN based on constraints analysis and satisfaction with higher mathematical modelling.



Graph 2: Comparative analysis of recall

Graph 2 depicts the Accuracy_values analysis on detection of DoS attacks by applying different ML/DL algorithm such as Decision Tree (DT), Random Forest (RF), CNN and FST-CNN.



Graph 3: DoS attack detection analysis

Using Graph 3, it is established that the security of FST-CNN is higher than the security provided by DT classifier, RF ensemble classifier and CNN deep classifier. This enhancement in detection capability for DoS attack identification by FST-CNN is done to better explanation-based reasoning, mobility and fuzzy based deductive inference modelling in FST-CNN.

CONCLUSIONS

The rapid evolution of the Internet of Things (IoT) has transformed modern communication and computing systems by enabling billions of devices to sense, process, and exchange information in real time. Within this ecosystem, Wireless Sensor Networks (WSNs) play a central role, offering distributed intelligence for applications such as smart healthcare, industrial automation, environmental monitoring, and intelligent transportation systems. However, the open and resource-constrained nature of WSNs makes them highly vulnerable to a range of security threats, including data tampering, packet drop attacks, Sybil attacks, and denial-of-service attempts. These attacks not only compromise network performance but also erode the trustworthiness of transmitted information, undermining the reliability of IoT-driven services. Against this backdrop, the present study explored the integration of deep learning-based intrusion mitigation with trust-aware routing mechanisms to enhance both the security and efficiency of IoT-WSNs. This work established that conventional cryptographic methods and lightweight anomaly detection systems are insufficient to address sophisticated intrusions, particularly those that evolve dynamically and mimic legitimate node behaviors.

REFERENCES

1. *Laila Tageldin et.al. (2025), "Internet of Things Security: Threats, Recent Trends, and Mitigation Approaches", Advances in Internet of Things, issn: 2161-6825, vol. 15, pages. 1-15.*
2. *Malliga Subramanian et.al. (2025), "Deep learning-driven methods for network-based intrusion detection systems: A systematic review", ICT Express, issn: 2405-9595, vol. 11, issue. 1, pages. 181-215.https://doi.org/10.1016/j.icte. 2025.01.005*
3. *M. Sakthimohan et.al. (2024), "Secure deep learning-based energy efficient routing with intrusion detection system for wireless sensor networks", Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, issn: 1875-8967, vol. 46, issue. 4, https://doi.org/10.3233/JIFS-235512*
4. *Deny. J et.al. (2024), "Secure deep learning-based energy efficient routing with intrusion detection system for wireless sensor networks", Journal of Intelligent & Fuzzy Systems, issn: 1875-8967, vol. 46(23), pages. 1-17. DOI:10.323 3/JIFS-235512*
5. *A. Merline et.al. (2023), "Progressive Transfer Learning-based Deep Q Network for DDOS Defence in WSN", Computer Systems Science and Engineering, issn: 2994-3205, vol. 44(3), pages. 2379-2394. DOI:10.32604/csse.2023.027910*

6. *Ahmad Y. Javaid et.al. (2017), "A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)", sesa, issn: 2693-2466, vol. 17(12), http://dx.doi.org/10.4108/eai.28-12-2017.153515*
7. *Ahmed Kamal et.al. (2005), "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Wireless Communications, issn: 1558-0687, vol.11(6), pages. 6-28. DOI:10.1109/MWC.2004.1368893*
8. *A.A. Zaidan et.al. (2017), "A review of smart home applications based on Internet of Things", Journal of Network and Computer Applications, issn: 1095-8592, vol. 97, pages. 48-65. https://doi.org/10.1016/j.jnca.2017.08.017*
9. *André Reichstaller et.al. (2018), "Optimization of global production scheduling with deep reinforcement learning", Procedia CIRP, issn: 2212-8271, vol. 72, pages. 1264-1269.https://doi.org/10.1016/j.procir.2018.03.212*
10. *Antonio G. DiPasquale et.al. (2016), "TAMEisoquin, a novel tripodal fluorescent zinc sensor with high Zn(II) affinity and Zn(II)/Cd(II) selective fluorescence response: Synthesis, coordination geometry, spectroscopy, and comparative response to biometal ions", Polyhedron, issn: 1873-3719, vol. 109, pages. 147-153.https://doi.org/10.1016/j.poly.2016.01.024*