*International Journal of Computational and Experimental Science and ENgineering (IJCESEN)*

*Vol. 10-No.4 (2024) pp. 1462-1474*
*http://www.ijcesen.com*

***ISSN: 2149-9144***



**Research Article**

# Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection in Wireless Sensor Networks

**Kosaraju Chaitanya[1,2*], Gnanasekaran Dhanabalan[3]**

[1]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai600062, Tamil Nadu, India.
[2]Department of Computer Science and Engineering, Vignan's Nirula Institute of Technology and Science for Women, Pedapalakaluru, Guntur522005, Andhra Pradesh, India.
* **Corresponding Author Email:** kchaitanyaveltech@gmail.com - **ORCID:** 0000-0002-7453-4377

[3]Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai600062, Tamil Nadu, India.
**Email:** gdhanabalan@veltech.edu.in- **ORCID:** 0000-0003-3462-7920

**Article Info:**

**DOI:** 10.22399/ijcesen.613
**Received :** 11 November 2024
**Accepted :** 22 November 2024

**Keywords :**

Wireless Sensor Networks,
Node Information,
Lightweight Cryptography,
Node Authentication,
Network Security.

**Abstract:**

A Wireless Sensor Network (WSN) is a network of low-power, networked sensors that may gather data for a range of applications. These networks rely heavily on energy and security considerations that are essential to their administration. Lightweight cryptography procedures are necessary to attain high levels of security in WSNs because the conventional security approaches are inappropriate due to the restricted resources of the nodes. Topology maintenance and attack protection for individual sensor nodes is impractical. When it comes to monitoring and data collecting, WSNs are frequently used in unattended and hostile environments. Deploying sensor nodes in such an environment leaves the sensor network vulnerable to malicious node insertion since it lacks physical protection. The next step is for an attacker to use malicious nodes to perform a variety of attacks that disrupt network connectivity. In these types of attacks, the malicious node pretends to be a legitimate node by dropping packets at random to evade detection. There are a lot of systems out there for detecting malicious nodes, but only limited models can actually identify assaults. A plethora of sensors and actuators are necessary to enable the automation of modern industrial processes. Prevention of authenticity fraud and non-repudiation is crucial for building trust and identifying data errors in this network. An effective asymmetric-key-based security mechanism is proposed in this paper for distributed cooperative networks that allows all nodes, including the gateway, to establish authentication and non-repudiation with different session keys that can be used for one time usage for authentication and for data security. Assuming there are no malevolent nodes, the approach also provides anonymity and confidentiality. Authentication and non-repudiation are still intact in the event that a single node is hacked. There will be little effect even if additional nodes are compromised. Using the authentication mechanism, this main security architecture prevents incursion from external hostile nodes. This research proposes a Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection (PNA-DSKS-NPA-MND) that is used for accurate node authentication and also for malicious node detection to increase the Quality of Service (QoS) levels in WSN. The proposed model when compared with the traditional models exhibits better performance in node authentication accuracy and also in detection of malicious nodes in the WSN.

## 1. Introduction

In a WSN, there are several independent sensor nodes that communicate with one another wirelessly, in other words, every sensor in the network is linked to at least one node [1]. Application requirements dictate the WSN design. In environmental monitoring, a network of sensor nodes covers an area, and then the data collected from all those nodes is sent to a central location, called a sink, where the rest of the processing can be done [2]. For these kinds of uses, sensor nodes are typically built to

operate in environments where it is not feasible to charge or replenish their batteries [3]. Therefore, energy is a resource that sensor nodes greatly value. Designing routing protocols becomes a daunting undertaking due to this restriction. The sensor nodes that make up the WSN can range in number from a few to hundreds or even thousands, with each node linked to a sensor or sensors [4]. A radio transceiver, an electrical circuit, a microprocessor, and a power supply are some of the components that make up a sensor node [5].

The nodes that make up a wireless sensor network are often placed in close proximity to or inside the event itself. Essentially, it's a network of autonomous devices spread out across a geographic area that work together to keep tabs on various physical or environmental factors. Security measures are necessary to guarantee the authenticity and privacy of sensitive data in WSNs since these networks might function in potentially dangerous environments [6]. Although it differs significantly from more conventional security mechanisms, WSN security is an essential area of study. This is due to the fact that, firstly, these devices are severely limited in their energy, communication, and computing capacities, among other areas. Second, there's always the chance of physical attacks like manipulating or capturing nodes [7]. The wireless sensor network model is shown in figure 1.

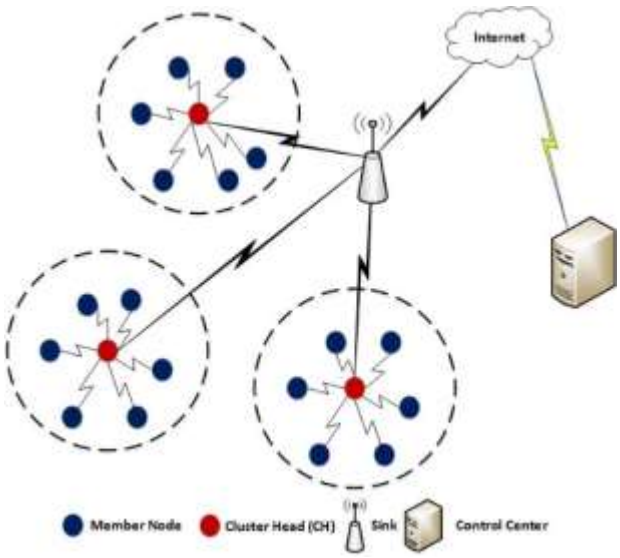


***Figure 1.*** *WSN Model*

Detecting the malicious node, such as through acknowledgement and multipath forwarding, requires a significant amount of communication resources. When implanted in their surroundings, wireless sensor networks can gather data [8]. Sensor nodes often do initial processing on the data before sending it to the sink node for additional processing via insecure channels [9]. Environment monitoring, public safety, healthcare, transportation, infrastructure management, medical, home and office security, and combat surveillance are among the many potential uses for sensor networks [10]. The importance of these programs makes them easy targets for cybercriminals. An attacker can target a WSN in several ways. One example is the practice of spoofing a message's fields while it is in route; this allows one to send an altered version of the original message to another recipient [11]. It is also possible to change a node's behavior by manipulating its hardware and/or software. The best defenses against various threats will vary in kind.

To ensure the privacy, authenticity, and integrity of sensed data and sensor nodes, cryptography is one of the many security protection technologies for WSN that are now accessible [12]. Simply said, cryptography is a collection of methods for encoding data such that only the intended receiver can decipher it. This is in contrast to the original, unprotected data. Node authentication and data encryption in cryptography typically makes use of security keys, which offer some leeway in the encryption and decryption process but also raise some difficulties about key management [13]. Choosing the most suitable algorithms is an important design decision in cryptography because algorithms based on different mathematical formulas and using different techniques will usually have different performances in terms of memory costs, processing power, and attack resistance [14].

It is common for sensor nodes in WSN to face limitations in processor power, memory, sensing capabilities, and energy supply, among other resources [15]. The WSNs have benefited from more powerful sensor motes made possible by new, inexpensive technologies. However, many current wireless multimedia sensor networks are likely to face limitations that make cryptographic techniques less useful [16]. Various methods for encrypting multimedia data have been suggested, with efficiency being a fundamental concern when implementing cryptography in wireless multimedia sensor networks [17]. WSNs provide unique security challenges because to the small size, low cost, and lack of processing power, memory, and battery life of the individual sensor nodes that make up the network. In order to circumvent the usage of computationally intensive public key methods, the majority of current security solutions for WSN rely on asymmetric key cryptography, which assumes that sensor nodes be pre-encrypted with secret, temporary startup keys [18]. Symmetric key cryptography isn't enough to guarantee wireless sensor networks are secure. Replenishing a functional wireless sensor network with more nodes in a secure manner remains an ongoing challenge.

The asymmetric cryptography model is shown in figure 2.

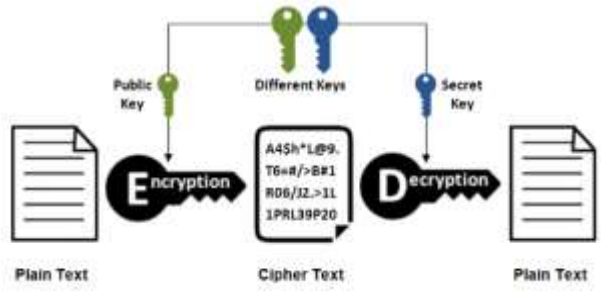


***Figure 2.*** *Asymmetric Cryptography*

Some encouraging findings have been found in recent studies on public key cryptography for WSNs, especially when it comes to elliptic curve and identity-based encryption [19]. Even while security is paramount for WSNs, certain security protocols have the potential to obstruct data aggregation and in-network data processing [20], two of the most important processes of a WSN. The key establishment, random key pre-distribution, data confidentiality [21], data integrity, and broadcast authentication is clearly discussed in this research [22]. Additionally, it reveals the limitations and issues associated with these solutions for WSNs. In addition, impressive progress made in WSN with public key cryptography is discussed. This research proposes a Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection that is used for accurate node authentication and also for malicious node detection to increase the QoS levels in WSN.

One of the many threats that WSN nodes face because of their openness is dishonest recommendation assaults, which provide the attacker misleading trust values. A fuzzy trust model and artificial bee colony algorithm (FTM-ABC) are the foundations of the suggested malicious node detection technique proposed by Pang et al. [1]. In order to determine indirect trust, the fuzzy trust model (FTM) is utilized. To enhance the trust model's ability to detect dishonest recommendation attacks, the ABC algorithm is employed. In addition, to improve effectiveness, the fitness function incorporates the recommended deviation and the interaction index deviation. Even when the number of dishonest nodes reaches 50%, the simulation results show that the upgraded FTM-ABC retains a low false-positive rate and a high recognition rate. As innovative wireless technologies and capabilities come into play, Unmanned Aerial Vehicles (UAVs) and the services they enable have the potential to greatly impact our day-to-day experiences. To deterministically identify the infected node deceiving the UAV flock, Zilberman et al. [2] suggested a method that integrates multi-path routing protocols with secret sharing and cheating identification algorithms. Even in the face of a skilled adversary that selectively alters data messages or reroutes them within the network, it guarantees a stealthy identification of the attacker offering fresh attack options. Following two fundamental criteria, the author ensured that this solution could be implemented in pre-existing networks. The author could only use standard routing protocols that were already in place, and the author could not rely on a centralized or trusted third party node, like a base station, to facilitate our solution. Each node must collect data exclusively from the preexisting primitives in the underlying communication protocols. The author demonstrated the cost bounds through thorough mathematical proofs and demonstrated feasibility through simulations. The simulations also demonstrate a flawless delivery and detection rate of 100%.

The objective, purpose, or movement of the driver, as well as the road layout, determine the network topology in Internet of Vehicles (IoV). The IoV presupposes that all vehicles have onboard computers, storage devices, and communication devices that can process data, store data, and interact with other vehicles and roadside infrastructure (RSI). To ensure that only legitimate data is being propagated in the IoV, data authentication is crucial. Therefore, safety is paramount in IoV. Some of the problems with strong security in IoV that have been discussed so far include inefficient communication, security without privacy, security that isn't dependable, and long delays caused by security algorithms. In order to solve these problems, Safavat et al. [3] suggested a routing system called ACO-AODV that uses Elliptic Curve Cryptography (ECC) to prevent messages from being spread by suspicious vehicles in the IoV. To be more precise, the suggested protocol has three parts: a certificate authority (CA) that uses ECC to encrypt publicly available data like license plates, an algorithm for detecting malicious vehicles (MV) that uses trust levels determined by interactions in status messages; and an adaptive system for secure optimal path selection based on communication intent using ACO-AODV to avoid malicious vehicles.

Security and energy consumption are two of the biggest issues with WSNs, which are characterized by their dynamic topology and restricted resources. Even while trust-based solutions are now practical for dealing with various node bad behaviors, issues including communication congestion, excessive energy consumption, and a variety of threats persist. So, to address these issues, Hu et al. [4] suggested a new system for routing data that is both secure and

energy efficient called TBSEER. TBSEER is able to withstand attacks such as black holes, selective forwarding, sinkholes, and hello floods because it determines the complete trust value by adjusting the direct trust value, the indirect trust value, and the energy trust value. On top of that, the harmful nodes are quickly identified using the adaptive penalty mechanism and the volatilization factor. To further decrease energy consumption caused by iterative calculations, the Sink obtains the indirect trust value and the nodes just need to calculate the direct trust value. With the comprehensive trust value in hand, the cluster heads may actively avoid wormhole attacks by finding the safest multi-hop pathways. According to the simulation results, the suggested TBSEER can withstand all typical threats, decrease network energy usage, and speed up the identification of malicious nodes.

The conventional knowledge about healthcare has been shaken up by the introduction of healthcare wireless medical sensor networks (HWMSNs). In HWMSNs settings, sensor nodes like wearable gadgets gather patient health data and send it to physicians for evaluation. A number of certificateless aggregate signature (CLAS) techniques have been proposed to ensure the confidentiality of patient information during transmission in HWMSNs. The use of a central key generation center (KGC), however, increases the likelihood of security breaches and privacy leaks. Coalition assaults that are both practical and destructive, brought about by an insider signer's collaboration with a malevolent KGC, are formidable foes. In order to address these issues, a system called CL-DVAAS, which stands for security-enhanced certificateless designated verifier anonymous aggregate signature, was developed by Li et al. [5]. The you-speak-once (YOSO) model proposes a committee that is both dynamic and unpredictable to take the place of the KGC during system startup and key distribution.

As wireless technology has progressed, mobile wireless sensor networks (MWSNs) have joined forces in a new application scenario to build intelligent cities that are innovative and to handle the many issues that come with security, adaptability, and resilience. To achieve confidentiality, integrity, and authentication and hence prevent harmful cyber attacks and resource abuses, one of the key techniques for MWSNs is to exploit lightweight cryptosystems. Protecting MWSNs is possible with the Saturnin lightweight cryptosystem, which will be showcased at ToSC 2020. Even if attackers are most vulnerable in a ciphertext-only attack, Saturnin does not appear to be able to withstand such an assault, according to the research. In this attack scenario, Li et al. [6] suggested a new statistical differential fault analysis (SDFA) using the square Chi-maximum probability estimate and Dice-Hamming weight as two distinguishers. After the tests were over, it used 656 mistakes in the last round of Saturnin to retrieve the 256-bit secret key. The innovative SDFA can cut faults in half with a reliability of at least 99% and expand fault injections to the deeper round, in comparison to the standard statistical fault analysis.

The privacy and security of the Industrial Internet of Things (IIoT) relies on the certificate-based aggregate signature (CBAS) scheme. To build an efficient data aggregation protocol, Qiao et al. [7] presented a concrete construction of the CBAS scheme that does not involve bilinear pairing. The primary argument of this piece is that the prior CBAS method was unable to deliver the promised security. Because it knows the master secret key, a malevolent KGC can generate a genuine forging signature. Following that, the author went over several concrete forgery attacks that might be used against current CBAS methods, proving that the prior related structures were insecure. The author also offered a real implementation of the proposed way to enhance the CBAS scheme, with the goal of further providing a secure CBAS scheme for IIoT. Proof of the novel proposal's security can be made in the random oracle model using the discrete logarithm problem's hardness. The architecture outperforms earlier CBAS methods in terms of security while being computationally and communicationally efficient.

The paradigm shift from a single large drone to several small drones linked together in an ad hoc fashion is marked by the growth of Flying Ad-hoc Networks (FANETs). Efficient resource utilization is key for FANETs to sustain QoS in multi-hop networking schemas. Unfortunately, FANETs are susceptible to malevolent nodes that can breach the network and cause significant security vulnerabilities, especially at the Medium Access Control (MAC) layer, because of the open wireless boundary and the great mobility of the drones. This vulnerability causes harm to the information exchange operation within the network and threatens the security and privacy of the network. An attacker can compromise the network's control in a number of ways: by sending out a flood of reservation requests, which will use up all available bandwidth; by listening to control messages; by using power-efficient jamming; or by providing false information. Consequently, a system for key agreement and safe access control are necessary. To protect itself from these threats, the mechanism has to use both the node authentication and key agreement phases. Khan et al. [8] presented a certificate-based approach for key agreement and access control that uses a one-way cryptographic hash function that is collision-

resistant and is based on the Hyperelliptic Curve Cryptography (HECC) technique. The suggested scheme is evaluated for its feasibility and performance by means of formal security analysis methods, including the Real-Or-Random (ROR) model and the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Sensors and actuators, which often have limited resources, can now connect to the Internet through the IoT. Encryption, message authentication codes, authentication, etc., are defense measures that must be utilized because it is susceptible to multiple security risks and attacks. Secure communication with and data collection from a group of devices is necessary for many IoT scenarios. It is important to efficiently update the group keys, which are required for multicasting information inside the group, in dynamic IoT environments since devices join and exit groups at random. For effective Group Key Management, Sudheeradh et al. [9] offered a new approach that uses factorial trees and the Chinese Remainder Theorem. Ensuring forward and backward secrecy, this proposed approach efficiently updates the group keys as devices join or leave a group and prevents unauthorized users from obtaining group information. The author demonstrated that the suggested scheme beats previous work's schemes in terms of the communication and computation expenses experienced by IoT devices after doing thorough mathematical analyses and numerical simulations to assess its performance.

The self-configuring Wireless Ad hoc Networks (WANET) for the IoT are known as WSN. These networks comprise a large number of resource-constrained Sensor Nodes (SN). Efficiency in energy consumption and safety are critical aspects in WSN. The presence of Malicious Nodes (MNs) makes it possible for the adversary to transmit erroneous information. It is critical to identify and isolate certain MNs in order to avoid security issues. As a result, Kumar et al. [10] proposed a method for identifying MNs in WSN by making use of the properties of each SN. In addition to addressing security concerns, this study provides energy-efficient data transmission (DT) by selecting the Cluster Head (CH) based on the remaining energy of the sensor. The Malicious Nodes Detection (MND) phase involves the Improved Deep Convolutional Neural Network (IDCNN) identifying and isolating MN into the malicious list box. During the energy-efficient DT phase, the Trusted Nodes (TN) are clustered using the Extended K-Means (EMM) algorithm. Then, depending on the residual energy of each cluster, an individual CH is selected using the t-Distribution based Satin Bowerbird Optimization (t-DSBO) algorithm. The CH is responsible for transmitting the cluster's data to the BS. When one CH's energy drops below a certain threshold, the t-DSBO switches to the other.

## 2. Material and Methods

### Proposed Model

There are four distinct kinds of security threats that could target wireless sensor networks: interruption, interception, modification, and creation. Interception compromises secrecy, interruption attacks compromise availability, alteration biases integrity, and fabrication impairs authentication. While there may be variances according to the nature of the program, these are the main threats [23]. So, their effects will be proportional to the severity of the damage that a security requirement impairment could do to the applications. The goal of an interruption attack might be to disrupt communication or to disable sensor nodes. One option is to launch a denial of service attack, which lowers the quality of applications by flooding the network with harmful or irrelevant packets [24]. Nodes' processor, memory, and energy resources may be quickly depleted by Denial of Service (DoS) attacks because to the increased packet processing requirements. In addition, physical layer DoS attacks can disrupt the functioning of MAC layer protocols, which can have a devastating effect on WSNs [25].

Capturing sensor nodes opens the door to interception and modification assaults. False information can be intentionally created or stolen from, which lowers the standard of application monitoring. Particularly susceptible to tampering attacks that is, gaining physical access to nodes in order to alter their configurations are nodes located in outdoor areas [26]. Potential security risks in WSN can manifest at several levels of conceptual communication. Loops, packet redirection to hostile nodes, and dependability compromises are all possible outcomes of attacks on routing and transport-layer protocols [27]. Because they can worsen congestion, transmission latency, and energy consumption, attacks that cause packet retransmissions to an excessive degree are also highly detrimental. The dynamic session key set model is shown in figure 3. There may be inherently dangerous and difficult-to-evade risks in the application monitoring functions. In general, nodes' energy reserves can be quickly depleted and legitimate requests' service quality compromised by an invasion of intrusion-related sensing requests. Attackers could alter the prioritization of sensors by generating false events of interest or other malicious information if sensor nodes are linked with sensing priorities based on their ability to acquire relevant data [28]. This kind of attack is hard to spot, and it


***Figure 3.*** *Dynamic Session Key Set*

could have a disastrous effect on the reliability of the monitoring system. Due to its ability to guarantee adequate levels of security at very cheap cost, cryptography in WSNs may be necessary in many monitoring applications. But multimedia sensors can detect and communicate a lot more data in the form of images, videos, and sounds than scalar sensors can, which only retrieve little numerical values. Because of this, WSNs cryptography inevitably becomes more complicated and resource-demanding as the amount of data that needs to be encrypted and decrypted and also for node authentication increases. Cryptography is typically context-dependent, necessitating appropriate techniques, because to the inherent differences between image, video, and audio data.

Different algorithms can be used to perform symmetric or asymmetric cryptography, but in general, they both allow for secure data exchanges. In fact, there are benefits and downsides to both of them that need to be carefully considered for each use case. To summarize, asymmetric encryption uses a pair of keys to encrypt data, in contrast to the symmetric cryptography paradigm that specifies a single shared key for both operations. Performance and computational costs are directly affected by this specificity, which also directs the construction of the cryptographic methods. With symmetric cryptography, the most difficult part is figuring out how to safely distribute the key, even though it's easier to implement because only one key is needed for encryption and decryption. Asymmetric cryptography makes use of a public key which is known by every node to encrypt data and a private key which is utilized for node authentication and for decryption leading to increased processing time and memory use. However, more powerful sensor nodes have entered the scene as a result of multimedia sensing's popularity, which calls for stronger cryptography in WSNs.

Nodes in a wireless network can communicate with one another and share data through radio signals. By eliminating the need for cables, traditional wired networks can be deployed in environments that are unfriendly to them or in situations where mobility is essential. In a wireless ad hoc network, nodes are not bound to any certain physical location or set of protocols. Here, establishing a multi-hop radio network among the nodes is crucial to the communication process. Every communication system prioritizes security. Reliable communication requires authentication of every node in the network. Public key cryptography, message authentication codes, and many more authentication techniques are available. The majority of these systems have security flaws or are overly complicated. With the use of key distribution, a technique is presented in this research that can authenticate sensor nodes in wireless sensor networks. Each node in the network is authenticated by the Network Central Authentication Authority (NCAA). The proposed model architecture is shown in figure 4.

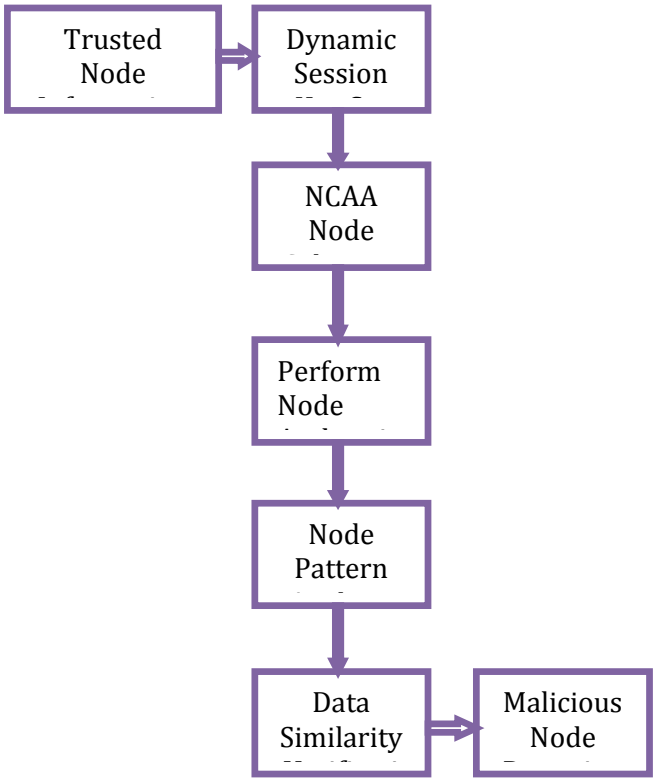


***Figure 4.*** *Proposed Model Architecture*

Similar to how cryptography keys are fundamental to data protection, management key approaches are also crucial. With a focus on constantly redeploying sensor networks and nodes' mobility, these approaches should facilitate the insertion and removal of nodes from the network. With the increasing complexity of cryptography in WSN settings, key management plays a crucial role in safeguarding data. A malicious node can selectively mimic the behavior of a legitimate node. As a result, malicious nodes transmit data at intervals that aren't typically used for transmission. It is possible to catch a malicious node at other common non-transmitting

times if it fails to transmit or pass data during non-transmitting hours. Neighbor nodes in the network can detect whether a malicious node transmits or relays data during non transmitting time, send empty packets to obfuscate their harmful intent. The network is alerted to the node's malicious conduct. Afterwards, the entire network stops communicating with the malicious node. Data from hostile nodes is not allowed by a sensor node. Neighbor nodes are able to easily identify the malicious nodes. This method of malicious node identification is thus reliable. This research proposes a Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection that is used for accurate node authentication and also for malicious node detection to increase the QoS levels in WSN.

**Algorithm PNA-DSKS-NPA-MND**

{

**Input:** Trusted Nodes Set {TNSet}

**Output:** Malicious Nodes List {MNset}

**Step-1:** The proposed model considers only trusted nodes in the network to involve in the communication process. The trusted nodes are the nodes whose performance is high in the network. The trusted node information processing is performed that is used to identify the nodes in the network. The process is performed as

$$TNproc[M] = \sum_{t=1}^{M} \frac{getnoderange(t)}{M} + getaddr(t) + \lambda(\max(t, t+1)) + \delta(t) \quad \{node \in TNset$$

Where getnoderange() model considers the nodes transmission range and getaddr() is used to identify the address of the node, λ is the transmission rate of a node and δ is the energy consumption of a node in the network.

**Step-2:** The proposed model makes use of asymmetric key model that generates the dynamic session key set. The dynamic keys are used to perform node authentication and also for accessing the data in the network. The dynamic session keys are used only in a particular session and cannot be reused. The dynamic session keys are generated as

$$SessionT[M] = \sum_{t=1}^{M} getTime(t) + Th$$

$$ValS[M] = \sum_{t=1}^{M} getVal(t)$$

$$ValR[M] = \sum_{t=1}^{M} getPrimeVal(t) \quad ValR > ValS$$

$$ValL[M] = \sum_{t=1}^{M} \frac{ValS(t) + ValR(t)}{2} \ll 2$$

$$Keypub[M] = \sum_{t=1}^{M} \frac{ValL(t) \oplus \mathrm{ValR(t)}}{ValS(t)||ValR(t)} + SessionT(t) + Th + \frac{ValR(t) \ll 2}{ValS(t)}$$

$$KeyPri[M] = \sum_{t=1}^{M} \frac{ValL(t)||\mathrm{ValR(t)}}{ValS(t) \oplus ValR(t)} + SessionT(t) + \frac{ValR(t) \ll 4}{ValL(t)}$$

**Step-3:** The NCAA node selection is performed based on the node trust levels and also based on the node performance levels in transmission, energy consumption and computational complexity levels. The NCAA node is used to monitor the nodes in the network and also to detect the malicious actions in the network. The NCAA node selection is performed as

$$NCAA = \sum_{t=1}^{M} \max\big(\lambda(t, t+1)\big) + \min\big(\delta(t, t+1)\big) + \min\big(dist(t, t+1)\big) + \max(\beta(t, t+1))$$

Where β represents the computational capability level of a node.

**Step-4:** Node authentication is the process of verifying the properties of node during transmission process. The node authentication is performed using the session keys. The node authentication allows a node to involve in transmission. The node authentication is performed as

$$Nauthen[M] = \sum_{t=1}^{M} getinfo\big(NCAA(t)\big) + getKeyPub(t) + G(SessionT(t)) \begin{cases} Nauthen \leftarrow 1 & if\ KeyPub == KeyPub(t) \\ Nauthen \leftarrow 0 & Otherwise \end{cases}$$

Here G is the model the calculates the session availability for key validation.

**Step-5:** Each node pattern is identified and the node properties are frequently monitored by the NCAA

node. The changes in node properties represent the cause of malicious actions in the network. The node pattern analysis is performed as

$$NPattern[M] = \sum_{t=1}^{M} \frac{\max(S(Packets(t))}{M} + \lim_{t \to M} \left( Nauthen(s) + \frac{\max(R(Packets(t))}{M} \right)^2 + diff(S(Packets(t)), R(Packets(t)))$$

**Step-6:** Each authenticated node can involve in data transmission process. The node pattern is analyzed and the data similarity levels are verified are regular time intervals. The change in data similarity indicates the intrusions in the network and the malicious nodes that cause data similarity variations are listed. The process is performed as

$$DSim[M] = \sum_{t=1}^{M} \frac{NPattern(S,R)}{M} + \frac{\sum_{t=1}^{M} simm(Packets(S,R))}{R(Packets(t))} + Nauthen(t)$$

$$MNset[M] = \sum_{t=1}^{M} TNproc(t) + \max\left(diff\left(DSim(t,t+1)\right)\right) + Nauthen(t) + \frac{\min(siff\left(NPattern(t,t+1)\right))}{M}$$

}

## 3. Results and Discussions

Each node in the WSN is powered by its own battery and has its own set of sensors, data processor, memory, and radio communication capabilities for short distances. These sensors are often scattered over the field at random. A wide variety of sensor nodes, such as those used for acoustic, seismic, and visual data collection, make up wireless sensor networks. Whether it's via multi-hop information communication, which involves sending data from one sensor node to another, or through single-hop information communication, which involves sending data directly to a base station, each sensor node in the system gathers data from the environment and transmits it. Whereever a WSN is implanted in its environment, it can gather data from there. As a rule, the sensor nodes handle data processing before sending it to the sink node, where it is delivered for additional processing via unknown channels. Environmental protection, transportation, public safety, medical, home and workplace security, and combat tracking are some of the many uses for sensor networks. The criticality of these systems makes them easy targets for attackers.

A WSN is vulnerable to multiple types of attacks. For instance, while a message is in transit, users might alter some fields so that the recipient receives a modified version of the original. Another way to alter a node's behavior is to exploit its hardware or software. Countermeasures must be tailored to the specific sorts of attacks. Potentially impeding the increasing utility of sensor networks are the inherent safety issues. There is a strong relationship between the area of fitness and this method. Consequently, the nodes are just as transparent as the case law. The cellular link for communication is still available to everyone. There are severe limitations on the nodes in terms of processing speed, data transfer rates, and battery life. Consequently, any hostile actor might initiate a series of attacks that could cripple the network in some way. For WSN security to be solved, a set of safety primitives that can make the network more stable and resilient should be implemented. A good illustration would be the need for encryption primitives in the construction of secure communication channels and the usage of key management systems in the distribution of the security credentials utilized by those primitives.

To ensure the security of sensor networks, cryptography is necessary. Cost, performance, and safety should all be carefully considered when designing a sensor, but doing so simultaneously is no easy feat. To save money, developers can forego acceptable security measures, such as those for key distribution, in favor of more affordable alternatives. More versatile approaches to key distribution are needed for a WSN. With a multi-hop transmission that ensures data confidentiality and integrity, WSNs should securely transmit data to a central node. Information loss, communication disruption, service slowing creating delays, and denial of service are just a few of the many attacks and threats that can target a WSN. The three primary security properties: authenticity, integrity, and secrecy are considered in this research. This research proposes a Precise Node Authentication using Dynamic Session Key Set and Node Pattern Analysis for Malicious Node Detection (PNA-DSKS-NPA-MND) that is used for accurate node authentication and also for malicious node detection to increase the QoS levels in WSN. The proposed model is compared with the traditional Malicious Node Detection Strategy Based on Fuzzy Trust Model and the ABC Algorithm in Wireless Sensor Network (MNDbFTM-ABC) and Statistical Differential Fault Analysis of the Saturnin Lightweight Cryptosystem (SDFA-SLC) in the Mobile Wireless Sensor Networks. The proposed

model exhibit better performance in accurate node authentication and detection of malicious nodes.

The proposed model considers the nodes information in the network. The nodes information helps in the identification of nodes in the network. The trusted nodes are only considered in the network for involving in data transmission process. The Trusted Node Information Processing Time Levels is shown in table 1 and figure 5.

***Table 1.*** *Trusted Node Information Processing Time Levels*

| Nodes in the Network | Models Considered | | |
|---|---|---|---|
| | PNA-DSKS-NPA-MND Model | MNDbFTM-ABC Model | SDFA-SLC Model |
| 50 | 7.7 | 16.5 | 18.5 |
| 100 | 7.9 | 16.7 | 18.7 |
| 150 | 8.0 | 16.9 | 18.9 |
| 200 | 8.2 | 17.1 | 19.0 |
| 250 | 8.4 | 17.3 | 19.2 |
| 300 | 8.5 | 17.6 | 19.4 |

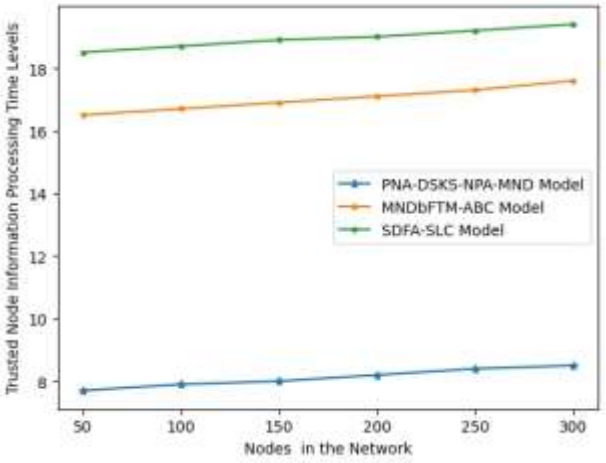


***Figure 5.*** *Trusted Node Information Processing Time Levels*

The proposed model generates a dynamic session key set that is used for node authentication and also used for information accessing to maintain security during data transmission process. The key set generated will wok for a particular session to avoid attackers to crack the keys. The Dynamic Session Key Set Generation Accuracy Levels are indicated in table 2 and figure 6. The proposed model initially considers the trusted nodes only to involve in communication process. The trusted nodes will also be verified for authenticity to check whether the trusted nodes turn into malicious.

***Table 2.*** *Dynamic Session Key Set Generation Accuracy Levels*

| Nodes in the Network | Models Considered | | |
|---|---|---|---|
| | PNA-DSKS-NPA-MND Model | MNDbFTM-ABC Model | SDFA-SLC Model |
| 50 | 97.5 | 94.6 | 93.3 |
| 100 | 97.7 | 94.8 | 93.5 |
| 150 | 97.9 | 95.0 | 93.7 |
| 200 | 98.1 | 95.2 | 93.9 |
| 250 | 98.3 | 95.4 | 94.0 |
| 300 | 98.4 | 95.6 | 94.2 |

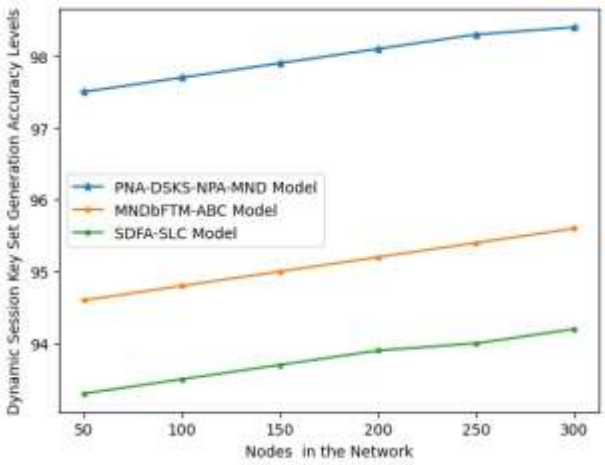


***Figure 6.*** *Dynamic Session Key Set Generation Accuracy Levels*

The node authentication helps to identify whether a nodes is a normal trusted or a malicious node. The Node Authentication Accuracy Levels are indicated in table 3 and figure 7. Each node data patterns are analyzed in the proposed model. The node pattern helps to identify the changes in the data contents to identify the malicious actions in the network. The node pattern will be done keenly to identify the minute changes also in the transmission process.

***Table 3.*** *Node Authentication Accuracy Levels*

| Nodes in the Network | Models Considered | | |
|---|---|---|---|
| | PNA-DSKS-NPA-MND Model | MNDbFTM-ABC Model | SDFA-SLC Model |
| 50 | 97.6 | 94.4 | 93.8 |
| 100 | 97.9 | 94.6 | 94.0 |
| 150 | 98.1 | 94.8 | 94.1 |
| 200 | 98.3 | 95.0 | 94.3 |
| 250 | 98.5 | 95.2 | 94.5 |
| 300 | 98.6 | 95.4 | 94.7 |

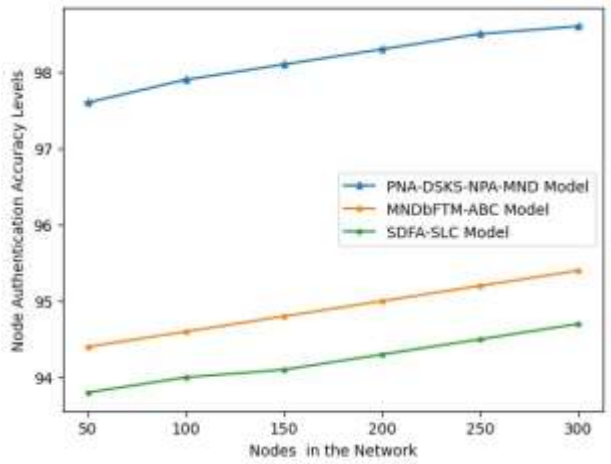


***Figure 7.*** *Node Authentication Accuracy Levels*

***Table 4.*** *Node Pattern Analysis Time Levels*

| Nodes in the Network | Models Considered | | |
|---|---|---|---|
| | PNA-DSKS-NPA-MND Model | MNDbFTM-ABC Model | SDFA-SLC Model |
| 50 | 13.1 | 17.6 | 20.5 |
| 100 | 13.3 | 17.8 | 20.7 |
| 150 | 13.5 | 17.9 | 20.9 |
| 200 | 13.7 | 18.1 | 21.1 |
| 250 | 13.8 | 18.3 | 21.3 |
| 300 | 14 | 18.4 | 21.5 |

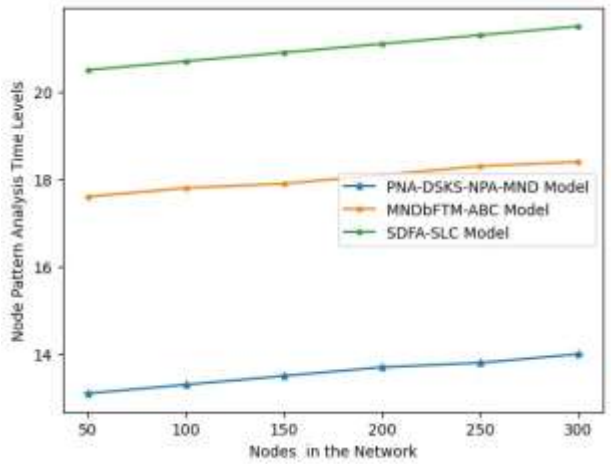


***Figure 8.*** *Node Pattern Analysis Time Levels*

The Node Pattern Analysis Time Levels are represented in table 4 and figure 8.

Data similarity checking is done at each node and each transmission will undergo data similarity levels. The integrity levels are detected using the data similarity check. The Data Similarity Verification Accuracy Levels are indicated in table 5 and figure 9.

***Table 5.*** *Data Similarity Verification Accuracy Levels*

| Nodes in the Network | Models Considered | | |
|---|---|---|---|
| | PNA-DSKS-NPA-MND Model | MNDbFTM-ABC Model | SDFA-SLC Model |
| 50 | 96.9 | 92.4 | 93.4 |
| 100 | 97.1 | 92.6 | 93.6 |
| 150 | 97.3 | 92.8 | 93.8 |
| 200 | 97.5 | 93.0 | 94.0 |
| 250 | 97.8 | 93.2 | 94.2 |
| 300 | 98 | 93.5 | 94.4 |

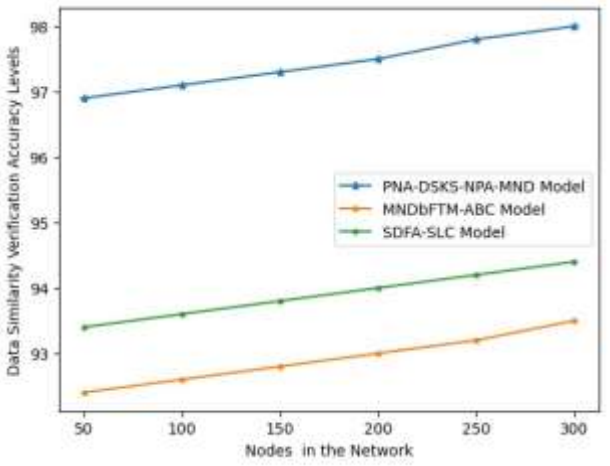


***Figure 9.*** *Data Similarity Verification Accuracy Levels*

The proposed model identifies the malicious nodes in the network by pattern analysis and similarity check. The malicious nodes that cause minute effect is also detected to increase the quality of service levels in the network. The Malicious Node Detection Accuracy Levels is depicted in table 6 and figure 10. The network security level is considered as the primary parameter that improves the effectiveness of the network. The network security levels increases the transmission rate, throughput levels in the network. The Network Security Levels are indicated in table 7 and figure 11.

***Table 6.*** *Malicious Node Detection Accuracy Levels*

| Nodes in the Network | Models Considered | | |
|---|---|---|---|
| | PNA-DSKS-NPA-MND Model | MNDbFTM-ABC Model | SDFA-SLC Model |
| 50 | 97.8 | 93.9 | 92.9 |
| 100 | 98.0 | 94.1 | 93.1 |
| 150 | 98.2 | 94.3 | 93.3 |
| 200 | 98.4 | 94.5 | 93.5 |
| 250 | 98.6 | 94.8 | 93.6 |
| 300 | 98.8 | 95 | 93.8 |

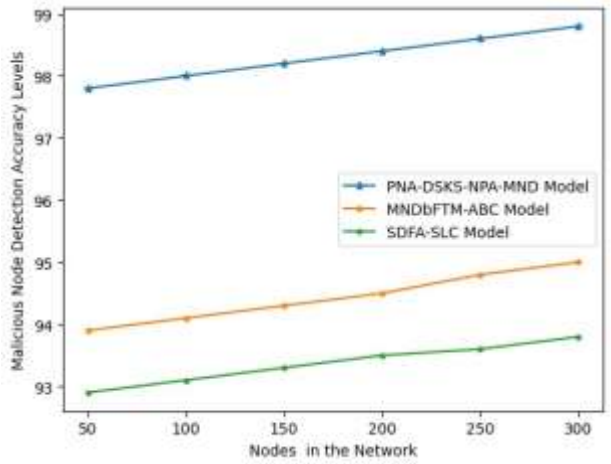


***Figure 10.*** *Malicious Node Detection Accuracy Levels*

***Table 7.*** *Network Security Levels*

| Nodes in the Network | Models Considered | | |
|---|---|---|---|
| | PNA-DSKS-NPA-MND Model | MNDbFTM-ABC Model | SDFA-SLC Model |
| 50 | 97.7 | 94.1 | 93.7 |
| 100 | 97.9 | 94.3 | 93.9 |
| 150 | 98.1 | 94.6 | 94.1 |
| 200 | 98.3 | 94.8 | 94.3 |
| 250 | 98.5 | 95.0 | 94.5 |
| 300 | 98.6 | 95.2 | 94.6 |

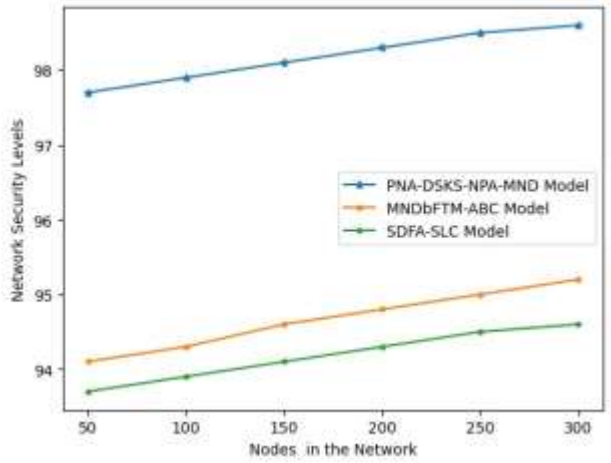


***Figure 11.*** *Network Security Levels*

## 4. Conclusions

Connected to a network of base stations, autonomous sensor nodes make up wireless sensor networks. The necessity for efficient security measures is driven by the fact that wireless sensor networks are becoming more susceptible to attacks as their user base expands. The restricted power, processing power, and storage space of individual sensor nodes makes it very difficult to determine an appropriate encryption for use in WSNs. When the number of sensor nodes rises, symmetric based cryptography algorithms do not scale well. This leads to the widespread use of schemes based on public keys. When collecting data or keeping tabs on a hostile environment, wireless sensor networks are frequently left unattended. Deploying a WSN in such an environment leaves it vulnerable to malicious node insertion since it lacks physical protection. There are a lot of systems out there for detecting bad nodes, but only a handful that can actually identify assaults. However, in order to detect rogue nodes, those suggestions waste energy and storage by sending duplicate messages. Locating hostile nodes in a network is a breeze using the suggested STL method. Very quickly, it identifies the rogue node. As a result, it helps dynamic sensor networks identify hostile nodes. In a network, a malicious node can be detected by a neighboring node. Locating it is not a difficult task. The capacity to detect rogue nodes in sensor networks is a key feature. The benefits and drawbacks of important pre-distribution strategies were illustrated. Given its potential as a public key approach, ECC is seen as a future key distribution implementation for WSNs since it might address issues that pre-distribution schemes did not fully address. We still haven't solved a few tough problems. Even using public key cryptography, it is still a challenge to add nodes to an existing network since all nodes in the dispersed network need to be notified about newly added and accepted public keys. In Identity Based Cryptography, the sink node is defined as a trusted third party, which helps with this problem to some extent. There are a number of traps that make revocation even more difficult. The first step is to determine whether a node is hostile or has been captured by an enemy. There aren't many studies that address this problem because identifying malicious nodes when they're acting legitimately and simply collecting traffic is next to impossible. Second, every node must be promptly sent the revocation packet, but bad nodes can act as black holes and block its delivery. The topics studied in this paper interesting and some other works done on it [29-34].

## Author Statements:

- **Ethical approval:** This article does not contain any studies with human participants or animals performed by any of the authors.
- **Conflict of interest:** The authors declare that they have no conflict of interest.
- **Acknowledgement:** The author is thankful to the supervisor Danabalan for his continuous support in completing the manuscript.

- **Author contributions:** The author K.Chaitanya developed the abstract, introduction, literature survey and proposed model and author Danabalan evaluated the results and concluded the manuscript.
- **Funding information:** There is no funding source for this research manuscript.
- **Data availability statement:** The data can be made available on request.

## References


[1] B. Pang, Z. Teng, H. Sun, C. Du, M. Li and W. Zhu. (Aug. 2021). A Malicious Node Detection Strategy Based on Fuzzy Trust Model and the ABC Algorithm in Wireless Sensor Network. *in IEEE Wireless Communications Letters*. 10(8);1613-1617, doi: 10.1109/LWC.2021.3070630.

[2] Zilberman, A. Stulman and A. Dvir. (2024). Identifying a Malicious Node in a UAV Network. *in IEEE Transactions on Network and Service Management*. 21(1);1226-1240, doi: 10.1109/TNSM.2023.3300809.

[3] S. Safavat and D. B. Rawat. (2021). On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities. *in IEEE Transactions on Intelligent Transportation Systems*. 22(8);5050-5059, doi: 10.1109/TITS.2020.3008361.

[4] H. Hu, Y. Han, M. Yao and X. Song. (2022). Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks. *in IEEE Access*. 10;10585-10596, doi: 10.1109/ACCESS.2021.3075959.

[5] X. Li, L. Zhou, X. Yin and J. Ning. (2024). A Security-Enhanced Certificateless Designated Verifier Aggregate Signature Scheme for HWMSNs in the YOSO Model. *in IEEE Internet of Things Journal*. 11(6);10865-10879, doi: 10.1109/JIOT.2023.3327505.

[6] W. Li, C. Liu, D. Gu, J. Gao and W. Sun. (2023). Statistical Differential Fault Analysis of the Saturnin Lightweight Cryptosystem in the Mobile Wireless Sensor Networks. *in IEEE Transactions on Information Forensics and Security*. 18;1487-1496, doi: 10.1109/TIFS.2023.3244083.

[7] Z. Qiao et al. (2023). An Efficient Certificate-Based Aggregate Signature Scheme With Provable Security for Industrial Internet of Things. *in IEEE Systems Journal*. 17(1);72-82, doi: 10.1109/JSYST.2022.3188012.

[8] M. A. Khan et al. (2021). An Efficient and Secure Certificate-Based Access Control and Key Agreement Scheme for Flying Ad-Hoc Networks. *in IEEE Transactions on Vehicular Technology*. 70(5);4839-4851, doi: 10.1109/TVT.2021.3055895.

[9] K. Sudheeradh, N. N. Jahnavi, P. N. Chine and G. S. Kasbekar. (2024). Efficient and Secure Group Key Management Scheme Based on Factorial Trees for ynamic IoT Settings. *in IEEE Access*. 12; 5659-5671, doi: 10.1109/ACCESS.2024.3350780.

[10] M. Kumar, P. Mukherjee, K. Verma, S. Verma and D. B. Rawat. (2022). Improved Deep Convolutional Neural Network Based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks. *in IEEE Transactions on Network Science and Engineering*. 9(5);3272-3281, doi: 10.1109/TNSE.2021.3098011.

[11] X. Gu, G. Zhang, M. Wang, W. Duan, M. Wen and P.-H. Ho. (2022). UAVaided energy-efficient edge computing networks: Security offloading optimization. *IEEE Internet Things J*. 9(6);4245-4258.

[12] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li and J. Wei. (2020). Survey on unmanned aerial vehicle networks: A cyber physical system perspective. *IEEE Commun. Surveys Tuts*. 22(2);1027-1070.

[13] Y. Lei, L. Zeng, Y.-X. Li, M.-X. Wang and H. Qin. (2021). A lightweight authentication protocol for UAV networks based on security and computational resource optimization. *IEEE Access*. 9;53769-53785.

[14] K. Rahman, M. A. Aziz, A. U. Kashif and T. A. Cheema. (2022). Detection of security attacks using intrusion detection system for UAV networks: A survey. *in Big Data Analytics and Computational Intelligence for Cybersecurity*. Cham, Switzerland:Springer, pp. 109-123.

[15] A.Rugo, C. A. Ardagna and N. E. Ioini. (2022). A security review in the UAVNet era: Threats countermeasures and gap analysis. *ACM Comput. Surveys*. 55(1);1-35.

[16] X. He, Q. Chen, L. Tang, W. Wang and T. Liu. (2023). CGAN-based collaborative intrusion detection for UAV networks: A blockchain-empowered distributed federated learning approach. *IEEE Internet Things J*. 10(1);120-132.

[17] L. Kong, B. Chen, F. Hu and J. Zhang. (2022). Lightweight mutual authentication scheme enabled by stateless blockchain for UAV networks. *Security Commun. Netw*. 2022.

[18] A.Kumar, Y. Singh and N. Kumar. (2022). Secure unmanned aerial vehicle (UAV) communication using blockchain technology. *in Recent Innovations in Computing, Singapore:Springer*. pp. 201-211.

[19] J. Shen, Z. Gui, X. Chen, J. Zhang and Y. Xiang. (2022). Lightweight and certificateless multi-receiver secure data transmission protocol for wireless body area networks. *IEEE Trans. Dependable Secure Compu*. 19(3);1464-1475.

[20] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos and S. W. Kim. (2020). The future of healthcare Internet of Things: A survey of emerging technologies. *IEEE Commun. Surveys Tuts*. 22(2);1121-1167.

[21] Peng, M. Luo, L. Li, K.-K. R. Choo and D. He. (2021). Efficient certificateless online/offline signature scheme for wireless body area networks. *IEEE Internet Things J*. 8(18);14287-14298.

[22] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han and C. Su. (2022). Blockchain-based reliable and efficient certificateless signature for IIoT devices. *IEEE Trans. Ind. Informat*. 18(10);7059-7067.

[23] J. Liu, L. Wang and Y. Yu. (2020). Improved security of a pairing-free certificateless aggregate

signature in healthcare wireless medical sensor networks. *IEEE Internet Things J*. 7(6);5256-5266.

[24] Y. Zhan, B. Wang and R. Lu. (2021). Cryptanalysis and improvement of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks. *IEEE Internet Things J*. 8(7);5973-5984.

[25] L. Deng, Y. Yang and R. Gao. (2021). Certificateless designated verifier anonymous aggregate signature scheme for healthcare wireless sensor networks. *IEEE Internet Things J*. 8(11);8897-8909.

[26] Y. Hou, H. Xiong, X. Huang and S. Kumari. (2021). Certificate-based parallel key-insulated aggregate signature against fully chosen key attacks for Industrial Internet of Things. *IEEE Internet Things J*. 8(11);8935-8948.

[27] F. Benhamouda et al. (2020). Can a public blockchain keep a secret? *Theory Cryptography*, pp. 260-290.

[28] Gentry et al. (2021). YOSO: You only speak once. *Proc. Adv. Cryptology–CRYPTO*, pp. 64-93.

[29] M. Devika, & S. Maflin Shaby. (2024). Optimizing Wireless Sensor Networks: A Deep Reinforcement Learning-Assisted Butterfly Optimization Algorithm in MOD-LEACH Routing for Enhanced Energy Efficiency. *International Journal of Computational and Experimental Science and Engineering*, 10(4);1329-1336. https://doi.org/10.22399/ijcesen.708

[30] M, P., B, J., B, B., G, S., & S, P. (2024). Energy-efficient and location-aware IoT and WSN-based precision agricultural frameworks. *International Journal of Computational and Experimental Science and Engineering*, 10(4);585-591. https://doi.org/10.22399/ijcesen.480

[31] Radhi, M., & Tahseen, I. (2024). An Enhancement for Wireless Body Area Network Using Adaptive Algorithms. *International Journal of Computational and Experimental Science and Engineering*, 10(3);388-396. https://doi.org/10.22399/ijcesen.409

[32] S, P. S., N. R., W. B., R, R. K., & S, K. (2024). Performance Evaluation of Predicting IoT Malicious Nodes Using Machine Learning Classification Algorithms. *International Journal of Computational and Experimental Science and Engineering*, 10(3);341-349. https://doi.org/10.22399/ijcesen.395

[33] Nennuri, R., S. Iwin Thanakumar Joseph, B. Mohammed Ismail, & L.V. Narasimha Prasad. (2024). A Hybrid Probabilistic Graph Based Community Clustering Model for Large Social Networking Link Prediction Data. *International Journal of Computational and Experimental Science and Engineering*, 10(4);971-982. https://doi.org/10.22399/ijcesen.574

[34] M, S., S, P., K, D., T, V., & D, B. (2024). Enhanced Energy efficient routing protocol for OnDemand distance vector routing to improve communication in border area Military communication. *International Journal of Computational and Experimental Science and Engineering*, 10(4);656-662. https://doi.org/10.22399/ijcesen.492