*Section : Research Paper*

# A Novel Authentication Protocol for Wireless Sensor Networks to Enhance Security with Energy-Efficiency

**G. Viswanathan**

Ph.D Research Scholar,

Department of Computer Science,

SNMV College of Arts and Science, Coimbatore, Tamilnadu, India.

Email: gviswanathanphdscholar@gmail.com

**Dr. M. Jayakumar**

Assistant Professor,

Department of Information Technology,

SNMV College of Arts and Science, Coimbatore, Tamilnadu, India.

**Abstract**

As a key component of the "Internet of Things (IoT)", "Wireless Sensor Networks (WSNs)" are becoming more crucial. For environmental observation, "Sensor Nodes (SN)" were dispersed randomly within WSNs. Deploying solely content-based security methods exposes WSNs susceptible to eavesdropping from both external and internal attackers in this kind of setting. Context confidentiality becomes an essential component of WSN security that should never be ignored since it could be used by an intruder to determine the location of the origin or even the "Sink Node (SiN)". There are several uses for WSN, which could be deployed to send confidential data. Implementing protective mechanisms to prohibit the attacker from compromising and revealing the origin and SiN's geolocation is crucial for keeping confidential material secure. Several traditional approaches for modeling privacy involve unnecessary computational complexity amongst SNs because of their restricted processing capacity, thereby impacting the WSN network's energy efficiency. Under this research, we suggest a new protocol called "Hashing Signature Code (HSC)" to solve the privacy concerns of traditional WSNs by striking a balance between the two competing criteria of

communication efficiency and resource consumption. The suggested HSC protocol authorizes SNs with the use of a "Pairing keys (PK)" conception mechanism. Only SiN and SNs have access to the proposed HSC system's special shared key entity. There is no need for a certificate-based authenticating scheme when working with two separate SNs to build a PK. The SNs inside a specific cluster have a common key. With its secure authenticating procedure, the proposed HSC security modeling can withstand clone and imposter threats. The proposed HSC protocol provides higher levels of security than the existing "Elliptic Curve Cryptographic (ECC)" method in terms of "Security Ratio","Energy Consumption Ratio", "Computation Time",and "Key Generation Time" as determined by the assessment methodologies used for both approaches.

***Keywords:*** *WSN, Security, HSC, ECC, Energy Efficiency.*

## 1. Introduction

WSNs eventually ensure the IoTis feasible, although widespread adoption of this system across sectors ranging from home appliances to defense has raised severe privacy concerns [1]. Connecting WSNs and certain other elements of IoT has benefits beyond mere wireless monitoring because multiple data sources could collaborate to deliver shared services [2].

Scientists predict that by the close of 2023, there will be more than "60trillion WSNs" being used around the globe.Despite its many advantages, integrating WSNs confidentially into the IoT poses significant difficulties.With limited battery and computing capabilities, WSNs were power-constrained networks [3].

The above makes them an easy target for hackers who would scrape up additional power than almost any other SN or "Base Station (BS)" could manage.In a conventional WSN network, thousands of SNs may be involved, each of which may be capable of either broadcasting or multi-hop transmission.WSNs are prone to safety threats due to the broadcasting structure of the communication system [4].

There have been 2 main categories of security protection methods in WSNs, which are known as "Data-Oriented (DO)", and "Context-Oriented (CO)", respectively.Data gathered by SNs including requests submitted to the WSN could be protected using a DO

technique.Contextual data, including the time and location of traffic patterns, is within the scope of a CO technique's classification of security [5].

As SNs were too large and undergo such consistent topological shifts, they operate autonomously but aren't generally subject to a centralized management body.Hence, conventional protective measures cannot be used since they introduce unnecessary complexity and resource consumption.Physically restricting accessibility to WSN SNs would be a primary line of protection against privacy breaches.Though many WSN applications require the installation of SNs throughout open, distant places that seem to be challenging to get to, manage, control, and protect from illegal physical entry, this seems to be problematic in WSNs [6].

The challenges of "Location Privacy (LP)" within WSNs stem from the fact that SNs possess unique characteristics, such as specified communication protocols and computing limits.Due to the transparent architecture of WSNs, adversaries might potentially listen in on transmissions and follow packets back to their points of origin as well as the SiN [7].

In a "CloningAttack", an attacker first steals a legitimate SN from the WSN and then sends sensitive information, including the detected SN’s key. The attacker then uses the extraction information to create various copies of that SN and calls them back to the WSN.In an"Impersonation Attack", an attacker can intercept the SNs from the WSN and obtain information from the detected SNs. Using this information, an attacker reflects detected SNs and puts duplicate SNs in the WSN [8].

This requires the provision of security mechanisms to prohibit the attacker from penetrating and so revealing the origin and SiN's position. While several encryption techniques have also been created to protect the privacy of transmitted data, attackers are also still able to get confidential material by exploiting the messages' circumstances [9].

As the hacker could see what's happening in the environment, keeping the LP of an origin is crucial. Events involving medical, defense, as well as other critical areas may cause this data to be difficult to discuss publicly. While the BS is crucial to the functioning of the WSN, it's likewise important to maintain the LP of a receiver. Whenever the SiN gets attacked and crashes, the entire WSN is rendered inoperable [10].

**Problem Statement:** The current security solutions in WSNs mostly implement cryptographic approaches which often generate overhead issues during intrusion detection in terms of higher resource utilization and energy requirements even though having the capability to resist attacks efficiently. Along with this, it is also found that most cryptographic and routing based security solutions are defensive to a specific form of attack which makes it unfeasible if the attack modeling gets changed concerning dynamic traffic conditions. Most conventional security modeling lacks efficiency during implementation as it generates additional computational overhead among SNs owing to its limited computational capability which significantly impacts the energy performance of the WSN.

**Paper Contribution:** The main objective of this proposed research work is to address the security problems of conventional WSNs by maintaining an equilibrium between the communication performance as well as resource requirement metrics. The contribution of this research is to introduce a novel computational HSC protocol modeling well capable of providing security solutions in data-driven WSNs with ease of efficient authentication in WSNs. The protocol model is designed and simulated using the NS2 tool environment, the authentication mechanism is developed in the form of an algorithm. It also discusses the extensive design analysis of the proposed HSC protocol with the existing ECC method followed by simulation outcomes, which justifies that the proposed solution obtains minimal resource constraints while achieving optimal security aspects in WSNs.

**Paper Organization:**Section 2 reviews some recent publications in WSN for secure data transmissions, Section 3 elaborates on the methodologies of the proposed HSC framework with crisp detail about the existing ECC framework for WSN security, and Section 4 discusses the implementation results obtained by both the existing ECC and the proposed HSC frameworks with its comparative analysis, and the research paper is concluded in Section 5 with future suggestions for more investigation.

## 2. Related Works

Protecting the location of a source from a nearby unauthorized party in WSNs was the motivation for the "SLPDR" approach introduced by the researchers in [11]. The terms "Cyclic Routing", "Greedy Routing", and "Directed Routing" are used alternately to characterize the several types of routing strategies it employs. The approach selects a starting SN at randomness from the network's edge. All services would first take the "Greedy Route",

then the "Directed Route" until finally arriving at the SiN. Its objective is to optimize data communication channels, and its routing pathways often have a constant duration and don't originate in a distant SN. This protocol was particularly very economical in terms of energy consumption because it employs a sufficient number of fake "Data Packets (DP)" to scare off an attacker without drastically decreasing the WSN's operational lifespan. The genuine DP has been buffered with a ring. An edge SN's false DP is swapped out for a genuine one when it passes through the ring on its way to the SiN. Nevertheless, this method lacks adequate security whereas if a hacker shows up on the same ring as the source SN.

The researchers of [12] presented a "Deferentially Private Framework" relying on a way of creating "Dummy Events (DE)" and then using those DEs to trigger the delivery of messages to predetermined SNs. In an attempt to render "Event Privacy Insensitive" to the involvement of specific SNs inside the "Event Reporting Process", this research proposed the idea of a location differentiation technique. It also shows that the initial part of the system may hide the true nature of the events by creating DE in such a way that the resulting traffic from either event is similar. In an attempt to conceal the occurrence of events through an energy-efficient manner, the network gets replaced with constant false traffic which replicates the real events using a periodic procedure. Then, they possess "Location Differential Privacy (LDP)", a method that protects and conceals events by generating traffic selectively. This method raises the level of uncertainty around the LP about an event thus giving only a little amount of assurance for it.

A "Secure Data Aggregation based on the Principle Component Analysis (SDA-PCA)" approach was proposed by the researchers [13].In this approach, a CH gets chosen among those nearby SNs based on the SNs' energy and their quality.To communicate with the SiN, the CH first collects data from sensors monitoring nearby SNs, compressing that data, and subsequently transmits it on.This protocol assumes that highly mobile SNs are typically harmful.Those SNs have been prohibited from advancing to the CH level.The SiN is protected against "False Event Messages (FEM)" through this method.It is simple to position a fraudulent SN such that it doesn't match the requirements for identifying whether an SN has been fraudulent because those conditions are straightforward.As a result, a bad SN might eventually become a CH.A CH's data could additionally be mostly unreliable.The proposed method cannot determine whether a CH generates a FEM because it trusts the CH's communications.

A "Secure Aggregation" mechanism in WSNs was suggested by the researchers [14]. Depending on connection quality and available energy, this protocol chooses a CH from among nearby SNs. Encrypted conversations amongst SNs and CHs, as well as CHs and SiNs, ensure that all sent data remains private. In addition, there is a "Unique-Key" for every SN and CH, which makes spoofing impossible. Whereas spoofing cannot be discovered when transmitting the information to the SiN because only the SiN has been able to recognize it. Consequently, compromising even a single SN enables a hacker to produce numerous FEM that is undetectable by the WSN.

A "Clustering Algorithm (CONsensus Based Data FIlteriNg for IIoT (CONFINIT))" was developed to stop FEM by the researchers [15]. Here, the sensory readings of every SN were compared with the values of the rest using this approach. An SN seems to be more probable to be fraudulent if its sensed data are notably different when compared to other SNs. In this scenario, legitimate SNs tend to avoid suspicious ones. In the interest of preventing malevolent SNs from creating FEM, the proposed approach employs several measures. Nevertheless, there isn't any way to identify FEMs at the transmitting SN or SiN, whereas if the fraudulent SN gets successful in creating a FEM, it'll remain undetected.

## 3. Methodologies

The methodology of the proposed HSC protocol is to design and develop a new computational paradigm for the security concern of a data-driven WSN where security solutions are provided during the "Data Aggregation (DA)" phase, when "Member Nodes (MNs)" are communicating with "Cluster Head (CH)", and CHs are communicating with the BS or SiN respectively. The following Figure 1 shows the architecture of the proposed design methodology.

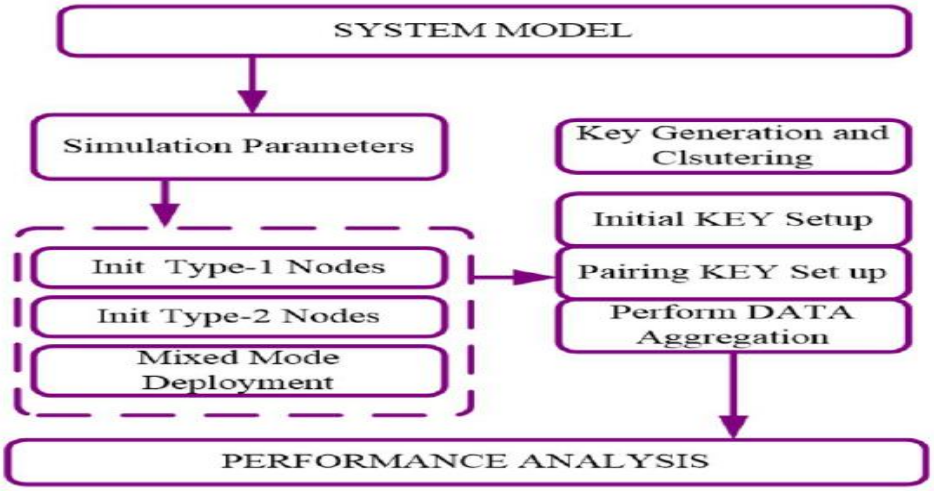


**Figure 1.** HSC Protocol Design Methodology

### 3.1. ECC (Existing Protocol)

In the existing, an effective key handling strategy for WSN with ECC has been developed. For the most part, a WSN could be considered to be made up of a substantial percentage of ordinary SNs (also acts as CHs) as well as a limited percentage of unique SNs.SNs that occur in clusters are far more powerful in parallel processing than SNs that occur in standalone.Each "Public/Private Key Pair" are perhaps generated earlier using an ECC-based key server, when the SNs are pre-distributed.ECC constitutes a form of "Public Key Cryptography", in which each communicating SN has its own "Pair of Keys (Public key/Private key)" as well as a corresponding operation set for performing cryptographic tasks.The "Private-Key" is unique to that SN, while the "Public-Key" is shared across all communicating SNs.It allows for encrypted communication across unsecured networks without the need for sharing private-keys.ECC is advantageous because its reduced key size necessitates less space for storing and transmitting keys while yet delivering the same degree of security as larger-key "RSA" approaches.Hence, a "256-bit ECC Public-Key" is expected to be just as secure as a "3072-bit RSA Public-Key". The "Point-Addition" and "Point-Doubling" ECC procedures serve the purpose of WSN security.The fundamental units of "Point Scalar Multiplication" are "Point Doubling".

**Disadvantages:**

- Under ECC architectures, "Uniprocessors" are used in SNs. Thus the "Multiprocessors/Multicores" cannot be used for parallel processing of repetitive tasks.
- The current generation of ECC uses a mode called "Cipher Block Chaining (CBC)" to keep information secure.A "Domain Decomposition Programming" paradigm, that might effectively ensure the effectiveness of parallel processing with "Multiprocessor/Multicore" platforms, is unavailable when using this method.
- There is no way for the interacting SNs to distinguish who is a real member and who isn't using authentication.Hence, "Cloning Attacks" could still operate against ECC.

### 3.2. HSC (Proposed Protocol)

The HSC system design phase as shown in Figure 1 comprises several stages wherein the initial phase of the proposed study formulates a "Mixed-Mode Deployer (MMD)" of 2 forms of SNs such as "N-1" and "N-2". The process involved in the MMD of SNs is as follows:

#### 3.2.1 . Design Phase (MMD of N-1 and N-2 SNs)

This section exhibits the strategy involved in defining a "Mixed-Mode Deployer (MMD)" paradigm to formulate WSNs by adopting two different types of SNs. The following "Algorithm-1 (A-1)" explains the MMD strategy.

**A-1: MMD**

**Start**
**Input:** (number of N-1 nodes) $\eta_1$, (Number of N-2 nodes) $\eta_2$
Where, $\eta \in Z^+$, *and* $\eta \neq 1$
**Output:** $f_{\text{Mix-Mode}}()$
1. Define deployment area A= [m×n]
2. Init $\eta_{\text{N-1}}, \eta_{\text{N-2}}$
3. Define boundary value Δ
4. Deploy x coordinate for each sensor node using a random distribution
$$X_i = \Delta + (A-2\times\Delta) \times f_{\text{rand}}(\eta_{\text{N-2}}, 1)$$
5. Deploy y coordinate for each sensor node using a random distribution
$$Y_i = \Delta + (A-2\times\Delta) \times f_{\text{rand}}(\eta_{\text{N-2}}, 1)$$
6. Generate a random orientation of N-1 nodes
$$\theta_{rand-type-1} = 2 \times \pi \times f_{\text{rand}}(\eta_{\text{N-1}}, 1)$$
7. Deploy mesh grid($x_i$,$y_i$)
8. Plot($f_{\text{Mix-Mode}}()$)
**End**

Figure 2 shows the outcome obtained after simulating the above stated process in a numerical computing environment where the MMD strategy has been adopted concerning a different number of SNs "Both for N-1 and N-2" with distinct characteristics. Figure 2 shows the MMD strategy where "η1"SNs and "η2"SNs are deployed within the "Area (100*100) unit$^2$" concerning"2-D Mesh Grid Vector". The next segment of thisresearch further initializes clustering followed by the DA process.

The proposed system considers the deployment of dynamicheterogeneous WSNs that consists of heterogeneous "Mobile SNs, and Static SNs (N-1 and N-2)" along with SiNs. It executes the PK establishment process before performing DA between SN to CH and from CH to SiN. The "N-2 SNs" characteristics are defined with higher computational capabilities whereas"N-1 SNs" characteristics pose comparatively lower system configuration setup as compared to the "N-2 SNs".

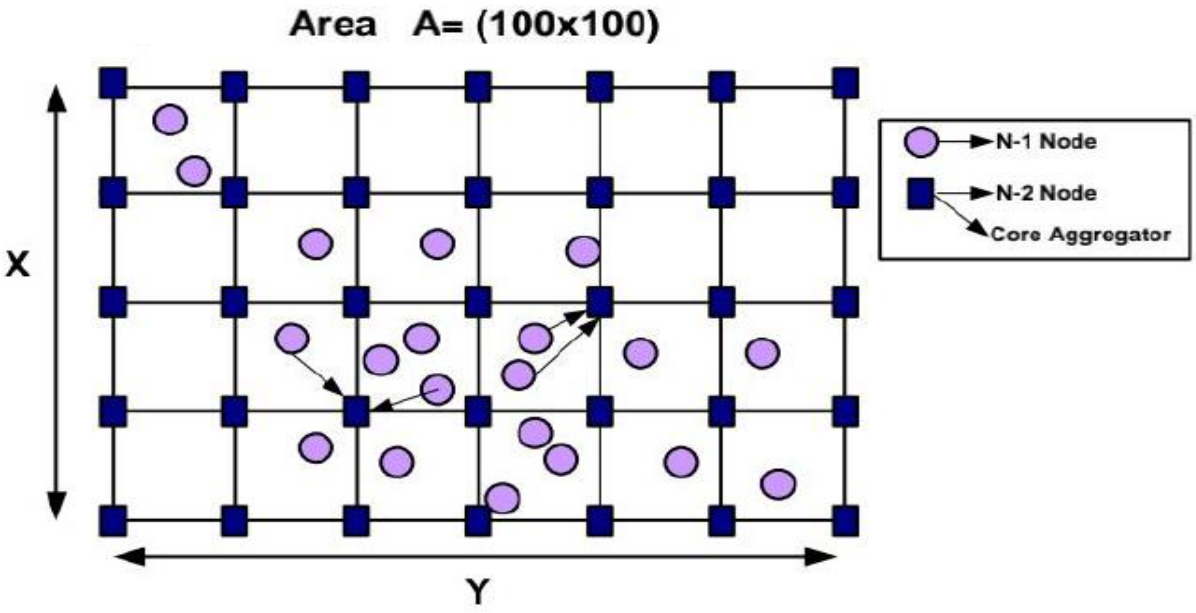


**Figure 2**. Strategy of MMD

In the proposed modeling "N-2 SNs" act as CHs and "N-1 SNs" nodes act as MNs. "N-1 SNs" get connected to the SiN mostly through "Multi-Hop", or "Single-Hop"communication. Each type of SN is identified with a unique ID.A "Key Entity Module (KEM)" which gets installed in CH or SiN mostlyperforms key management beforethe DA phase and also issues"Private/Publickey pairs"to each SN belonging to the network. KEM also issues certificates alongwith public and private key pairs for each SN in the network. The proposed HSC performs authorization of SNs by incorporating a PK generation process.

### 3.2.2. Assumption Phase (Adversarial Model Analysis)

The section formulates some assumptions before designing the security modeling of the proposed HSC system. It is anticipated that an intruder can perform a physical attack on the SN during the DA and transmission process where the SN is exclusively deployed to collect some secret/confidential information. The attacker SN can perform a lot of operations such as duplicating the captured SNs to colonize the network for malicious purposes and also it can perform an "Impersonation Attack" to mimic the behavior of a genuine SN. The attacker SN also can be programmed to execute various other forms of lethal security attacks such as eavesdropping, reply attack, etc. The prime reason behind performing those attacks is to compromise the confidentiality of data for malicious purposes.

***Therefore, the following are security requirements to design the proposed PK based modeling during DA in a dynamic environment***:

- An affected SN should not compromise or affect the security entities of other genuine SNs. It should not disclose the PK keys of other genuine SNs during the DA process when the communication happens between SNs to CHs and CH to a SiN.
- The proposed security modeling should comprise a unique feature that can resist "Cloning and Impersonation Attacks" by incorporating a secure authentication mechanism.
- The technique must have the features to obtain forward and backward secrecy paradigms to ensure efficient encryption and decryption of the message.
- It must have the ability to endure known-key attack modeling with mathematical computing features.

### 3.2.3. Initial Key-Generation Phase

The proposed HSC protocol applies a clustering paradigm among the SNs deployed for specific task execution. Further, it assesses a secure DA process integrated with HSC based authentication mechanism. ln the process of PK generation, each SN generates a unique pair of keys by combining unique, random public and private key components. The system attributes "Generation-($\propto$)" for each SN is executed by KEM installed at BS. The BS considers security attributes which are a set of "k-bit prime number", "Tuples-($t_1$, $t_2$)", "Hash-Function", "Public-Key", and "Root-Key". The "Algorithm-2 (A-2)" shows the modeling process for generating keys.

***The following process shows how initial keys are distributed before performing PK distribution:***

- The proposed HSC protocol utilizes a very unique key entity that is shared only between SiN and SNs.
- The PK establishment is considered between two individual SNs which do not require any certificate-based authentication schema.
- A "Group Key ($G_{key}$)" is distributed among the SNs belonging to a particular cluster.

**A-2: Initial Key-Generation**

**Start**

**Input:** $K_{size}$(bits)-prime $\eta \in Z^+$, a security parameter

**Output:** $f_{Inital\text{-}Key\text{-}Setup}()$

1. init $k_{size\text{-}prime}$
2. for i ← $2^k$: -1: 0
3. Check if round(i) is prime
4. break,
5. end
6. Determine system parameters $f_s[ t_1, t_2, t_3, t_4]$
7. Compute the master private key $M_{p\text{-}key}$
8. Compute public key $P_{pub\text{-}key} = M_{p\text{-}key} \times t_4$
9. Define cryptographic hash functions with different orientation
    1. $f(H_0) = f_{rand}(1,1) \times (t_3)^2$
    2. $f(H_1) = (t_3) \times f_{rand}(1,1) \times (t_3)^3$
    3. $f(H_2) = (t_3) \times f_{rand}(1,1) \times (t_3) \times f_{rand}(1,1) \times (t_3) \times f_{rand}(1,1) \times t_3$
    4. $f(H_3) = (t_3) \times f_{rand}(1,1) \times (t_3) \times f_{rand}(1,1) \times (t_3) \times f_{rand}(1,1) \times t_3$
10. Concatenate all the attributes
11. $f_{Inital\text{-}Key\text{-}Setup}()$ ← α **(list of system parameters)**

**End**

During the generation of system parameters, the SiN runs KEM and generates "$M_{p\text{-}key}$" which is further kept as a secret, and the "Concatenated System Parameter (∝)" gets published among individual SNs. After generating the system parameters, SN assigns a "Unique Identifier" to "N-2 SNs" which are denoted with "$ID_{N\text{-}2}$" and also assigns a "Unique ID ($ID_{N\text{-}1}$)" to "N-1 SN".

The proposed HSC protocol further initializes a list of "Legitimate Nodes ($L_{legit\text{-}nodes}$)" which is maintained in the SiN. This process controls the individual operations in between "N-2 SNs" which are having a comparatively higher computational capability. It also initializes "Partial Public and Private Key" entities for individual SNs which are deployed within the above highlighted region in Figure 2.

Further, each SN identifier can validate its individual "Private-Key" and also can compute its full associative private and public key components. The certificate-less PK in this context refers to entities that are generated by KEM before deploying the WSN. It is exclusively meant for individual SN performance with mutual pairwise authentication before activating the DA process.

The entire set of "N-1", and "N-2" SNs also maintain their respective individual key components to encrypt their respective data corresponding to any sensitive information, e.g., if an SN wants to transmit some control signal to the SiN then it can encrypt it with its individual SN key before transmission. Similarly, a SiN also can do so with its corresponding ID.

During the PK establishment process, the proposed protocol applies a secure schema to maintain secure communication using an authentication procedure. In this process, each SN shares its different PK with its adjacent SNs for security means. For example, Core aggregator SNs or CHs can make use of this schema. If an SN having the limited computational capability, i.e. "N-1 SN" wants to become an MN of a new cluster then it should share its PK with "N-2 core aggregator SNs". On the completion of this process, the core-aggregator SN can encrypt its cluster key, which is usually used to secure the broadcast messages within its respective cluster using PK components. Similarly, "N-1 SN" can securely encrypt its sensitive data using its PK and then transmits it to its respective CH using certificate-less PK generation and distribution. An "N-2 CH" maintains the list of "Cluster-Keys" and also tracks down whether an "N-1 SN" joins or leaves the cluster.

The proposed HSC protocol also performs individual key generation by incorporating an authentication schema where "Individual Key Attribute ($Key_{ind}$)" is computed by simulating the function as given by Equation 1:

$$Key_{ind} = f_{HMAC}\,(z \times ID_{N\text{-}2}) \qquad \text{Eq}\rightarrow 1$$

When the key generation process is completed, the SiN initiates a list of legitimate and authorized member SNs concerning their identifiers and public key components. Every key attribute occupies a limited amount of memory in each SN.

**PK Generation Process**

- The modeling of PK generation utilizes multiple key parameters like keys of "Each SN, Public-Key, Secret-Key, and Encrypted-Keys". Initially, the system considers a list of "System Parameters ($\propto$)" and a selection of common "Secret-Key ($S_{key}$)" values.

- Further "Public Key ($P_{key}$)" is computed based on the product of a common "Secret-Key" and a "Tuple Element ($t_4$)".
- An empirical formulation is performed to obtain multiple hash functions to perform the computation of partial public/private key pairs. These key pairs are generated in the form of a matrix in which each SN holds its matrix value to obtain secure association among other SNs.
- During the computing of partial public/private key, all SNs have to perform the validation of their "Private-Keys" and after validation, the SN can further generate the "Full Private-Key". Here, the system can use cryptographic functions to generate a key for a particular SN.
- The next step performs the computation of PK based on the product of the SN security identifier and "Tuple Parameter ($t_4$)". Further, the model computes multiple different security parameters based on empirical formulation.

### 3.2.4. Cluster Formation and DA Phase

In cluster formation followed by the DA phase is composed of several other computational procedures where initially the proposed system performs SN discovery and authentication process which involves the above procedures such as generation of the PK.

- After the deployment of "N-1 and N-2 SNs", it exchanges beacon messages for authentication and form clusters.
- The SN discovery and authentication phase includes broadcasting of beacon messages which contain the ID of "N-2, N-1 SNs" and performs PK generation once each SN finds other SNs within their "Communication Radius (R)".
- All the respective distances are further computed and get the stored memory structure of the system. After that, each cluster generates and provides a "Cluster-Key" to its respective MN where the encryption has to take place before performing membership authentication.
- The proposed system allocates memory to the SN and CHs for updating the "Cluster-Key" and PK.
- The PK establishment process happens between two SNs that have shared a PK. As the proposed system incorporated a dynamic scenario where SNs are movable and can

join and leave a cluster at any time such that each CH maintains its respective memory to track down every particular activity associated with SN movement.

- After completion of key generation and PK set up the proposed system initiates secure DA in between MN to CHs and CHs to SiN.

### 3.2.5. Overall HCS Algorithm Work Flow

This section presents the proposed HCS algorithm which is exclusively designed to simulate and verify the above system modeling in a numerical computing environment. The preliminary design of the algorithm for the proposed work is being initialized using different simulation parameters such as "$T_{back\text{-}off}$, $T_{threhold}$", speed of SNs, and several simulations.

The system model is designed to work hierarchically by forming clusters of SNs in a specific way of membership classes, along with the process of performing an aggregation for all incoming data coming from the MNs of the clusters. The aggregation process performs message authentication by using the hashing process that plays a significant role in securing DA and authentication hand in hand. Finally, the hashing performs an encryption process and key authentication into a single process by taking all communication stages to ensure the integrity of data.

The numerical expression mentioned in Equation (2) shows the operation of padding operation considering both "inner padding (ipad)" and "outer padding (opad)" for the execution of the secure authentication operation to ensure data integrity by the function of "Crypto (hash)" with an "Input ($MP_{KEY}$)" and "Data (D)". The "N-2 CH" selection is considered based on the exclusive condition of the immediacy orientation where the "SNs N-1" present in the transmission range of the "SNs N-2". Therefore, during data aggregations as well as the clustering process each "MN (N1)" needs to ensure its integrity using sharing of the clustering key.

$$H - MAC\ (MP_{KEY}, D)\ \leftarrow\ H((MP_{KEY1} \otimes opad))\ ||\ H\ (MP_{KEY1} \otimes ipad\ ||\ D))\quad \text{Eq}\rightarrow 2$$

In a nutshell, the secure DA process takes place using the efficient message verification process beforehand passing it to any of the nodes either the member SNs or the cluster SNs that nullify the possibility of any falsification towards data integrity. The most interesting aspect of the designed model is that it has the flexibility of choosing the popular

"Hashing algorithm from the Hash Set (HS)-{"SHA-1", "SHA-256", "SHA-384", "SHA-512"}" depending upon the requirement of the size of the message blocks so that it balances the memory and processing overhead suitably along with the data priority.

The analytical system model performance behavior is validated using simulating it with the different system parameters in an iterative way and the time complexity behaviors analysis during the key generation and updating process in SNs as well as the cluster structure of the key pools. The model exhibits an optimal usage of energy and also consumes less computational resources in terms of memory and processing units as compared to the traditional counterparts, this shows the effectiveness of models for balancing both securities as well as optimization of resources to gain higher lifetime and mitigation of any kind of hard effects from the adversaries.

In addition, the models adopt a unique mechanism or process for the key generation with a key-value pairing, in this process, every SN has the capability of generating light-weight keys in a highly random way so that it becomes very hard for the intruders to perform any kind of attacks and further the composition of both private as well as public keys updates the key pooling. The model which is predominately designed as an authentication protocol suitable for an eco-system in WSNs suitable work with all the constraints of resources, this mechanism which is capable to work with all ensures that every data in transmission among the SNs are secured in the process of DA and transmission.

## 4. Results and Discussions

Using the "NS-2 Simulator", with a size of the network "1000m*1000m", both the proposed HSC as well as the existing ECC framework can operate in the military field. The WSN's SN has been positioned to observe the environmental's activity and uncover the military field records using highly secured standards. The sampling rate while carrying out the individual operation is "25 milliseconds". In the "Random Way Point (RWM)" paradigm, any SN moves individually within every route inside the shared network. When setting up a network, RWM typically employs an average SN count. Using the aforementioned counts and proportions, we can specify a location to go to at a random pace. In Table 1, we provide the simulation settings used to carry out the experiments. The modeling outcomes are achieved by utilizing numerous setups with repeated runs. Analyses of both the existing ECC

as well as the proposed HSC protocol's effectiveness are conducted. The correct measurements are used to assess the effectiveness comparison with help of tables and graphs.

**Table 1.** Simulation parameters

| Parameter | Value |
|---|---|
| Simulator | NS-2.31 |
| Network Coverage area | 1000m * 1000 m |
| Mobility framework | Random Waypoint model |
| Node movement (i.e, speed) | 25 m/s |
| Number of nodes | 10,20,30,40,50,60,70,80,90,100 |
| Connected Path link | Multi-direction |
| Packet rate | 8 packets/seconds |

**(i) Security Ratio (SR)**

A military's SR has been calculated as the percentage of their data that was transmitted securely relative to the overall amount of data. The SR calculated from military field records is most often expressed as a "Percentage (%)" and has been statistically constructed according to Equation (3). If military data has a greater SR, then the protocol is considered to work effectively.

$$\text{SECURITY RATIO} = \frac{\text{NUMBER OF MILITARY DATA SECURELY TRANSFERRED TO THE DESTINATION}}{\text{TOTAL NUMBER OF MILITARY DATA}} \quad \text{Eq}\rightarrow 3$$

**Table 2.** Security Ratio

| Average Military Data | ECC | HSC |
|---|---|---|
| 100 | 90 | 95 |
| 200 | 84 | 92 |
| 300 | 76 | 89 |
| 400 | 66 | 86 |
| 500 | 54 | 83 |

Table 2 shows the SR measure for different military field SNs' information for the proposed HSC protocol in comparison with the existing ECC protocol. The number of

military data in WSN is varied from 100 to 500. Table 2 and Figure 3 demonstrate that the HSC protocol improves the SR of military records over the existing ECC protocol according to its military records. When comparing the SR of the existing ECC to the SR of the proposed HSC considering 500 records, it is discovered that the proposed HSC protocol increases the SR of the military records over the existing ECC protocol.

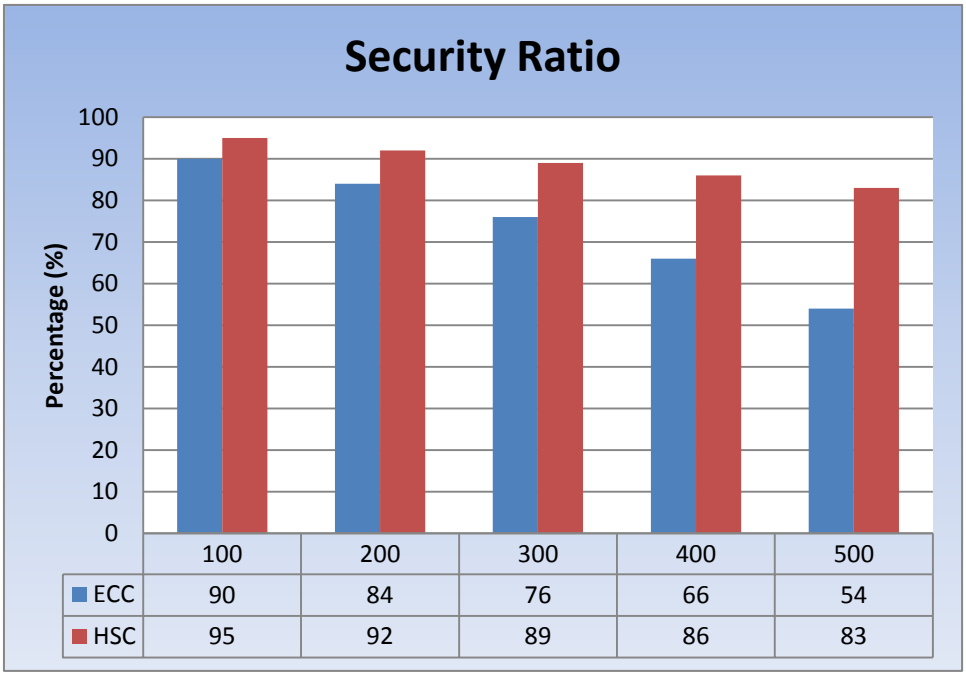


**Figure 3.** Security Ratio

**(ii) Energy-Consumption Ratio (ECR)**

When comparing the consumption of energy for a particular SN to the entire number of SNs inside a WSN, the HSC framework provides a measurement of the ECR for transferring military records from one SN to another. The ECR is expressed in terms of "Joules (J)" using the following Equation (4):

$$\textbf{Energy Consumption Ratio (ECR)} = \textbf{Individual SN Energy} * \textbf{Total SNs Energy} \quad \text{Eq}\rightarrow 4$$

Energy per single SN "$Energy_{SN}$" multiplied by the number of SNs inside the WSN networks "$Total_{SN}$" provides the ECR for reliable distant military operations as per Equation (4). Whenever the ECR remains minimal, then the protocol is considered to work better.

**Table 3.** Energy Consumption Ratio

| Total SNs | ECC | HSC |
|---|---|---|
| 20 | 1180 | 780 |
| 40 | 2360 | 1560 |
| 60 | 3540 | 2340 |
| 80 | 4720 | 3120 |
| 100 | 5900 | 3900 |

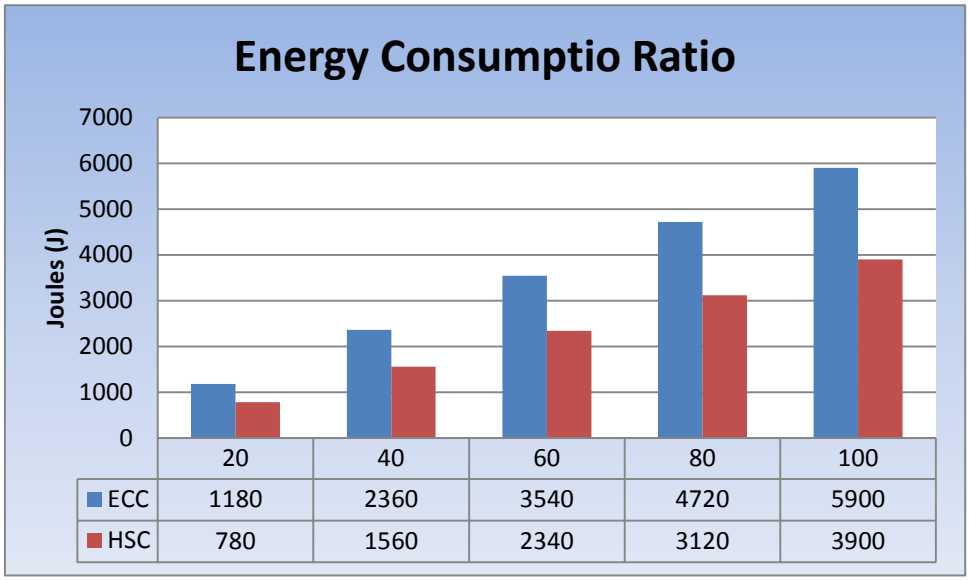


**Figure 4.** Energy Consumption Ratio

Table 3 shows the ECR for different military SNs' information for the proposed HSC protocol in comparison with the existing ECC protocol. The number of SNs in WSN is varied from 20 to 100. Table 3 and Figure 4 indicate that the HSCprotocol results in a lower ECR for SN than the existing ECC protocol. The ECR of the protocols varies from 780 joules to 5900 joules. Whereas SN has several 100, the proposed HSC protocol results in the consumption of 3900 J of energy for secure monitoring the military data whereas the existing ECC protocol results in the consumption of 5900 J. Hence, it is evident that the proposed HSC protocol results in a shorter ECR than the already existing ECC protocol. Figure 4 shows a visualization of the data from Table 3 in graphical form.

**(iii) Computation Time (CT)**

Time and storage needed by a protocol toward an input of a certain size are quantified by the CT.This is often done by calculating the convergence rate (the number of operationsrequired) or the memory requirement (the number of storage places required) of a protocol considering the size of its input, as indicated in Equation (5).Efficient protocols are

those whose values for this metric are minimal or rise slowly about the dimensions of the inputs.

$$\textbf{Computation Time} = \textbf{Amount of time for computing} * \textbf{Size of record data} \quad \text{Eq}\rightarrow 5$$

Table 4 shows the CT for different military SNs' record sizes for the proposed HSC protocol in comparison with the existing ECC protocol. The record size of SNs in WSN is varied from 20KB to 100KB. The results in Table 4 and Figure 5 show us that the Computational Time (Seconds) of the proposed HSC protocol is significantly lesser by the increasing proportion of "Data Size (KB)" and then compared it with the existing ECC protocol.

**Table 4.** Computation Time

| DataSize (KB) | ECC | HSC |
|---|---|---|
| 20 | 2.2 | 1.1 |
| 40 | 4.4 | 2.2 |
| 60 | 6.6 | 3.3 |
| 80 | 8.8 | 4.4 |
| 100 | 10.1 | 5.5 |

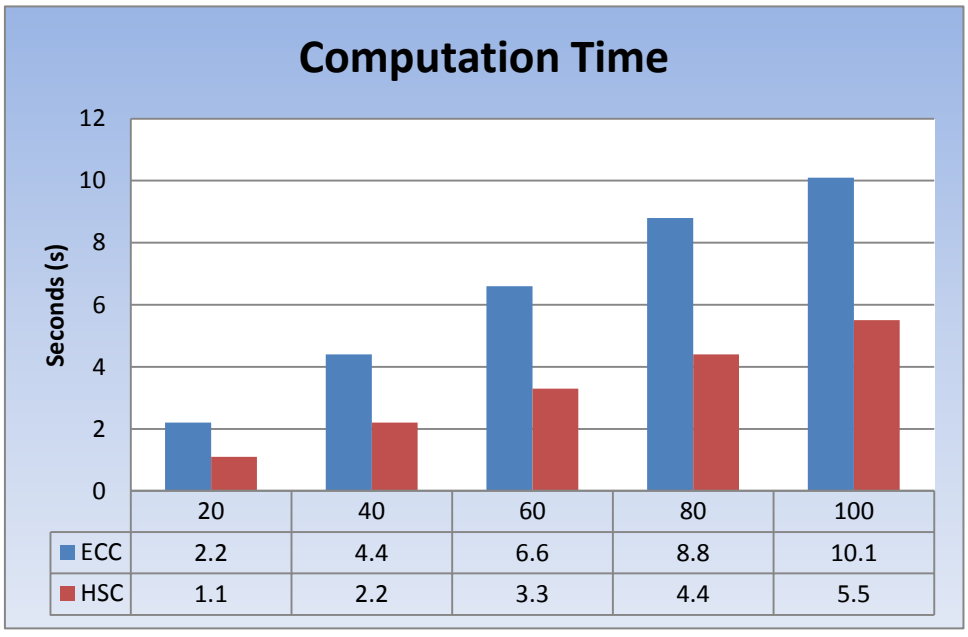


**Figure 5.** Computation Time

**(iv) Key Generation Time (KGT)**

The "Cluster-Key" update process executes when the "N-1 SNs leaves" or "Join New Cluster". If no "N-l SNs Leave or Join any Cluster" for a long time then, the CH will perform periodic updates considering frequent time instances for performing "Cluster-Key" updates. The proposed HSC protocol does not include any complex operation in the algorithm and is less associated with repetitive kind of processes in the security key establishment. Therefore, due to lightweight implementation, the system is quite faster responsive. The KGT is calculated in seconds when the number of SNs updated on the particular cluster as shown in Equation (6):

$$\text{Key Generation Time} = \frac{\text{Cluster Key Generation}}{\text{Join / Leave Clusters}} \qquad \text{Eq}\rightarrow 6$$

**Table 5.** Key Generation Time

| Number of SNs | ECC | HSC |
|---|---|---|
| 5 | 3.4 | 1.7 |
| 10 | 6.8 | 3.4 |
| 15 | 12.16 | 6.8 |
| 20 | 24.32 | 12.16 |
| 25 | 48.64 | 24.32 |

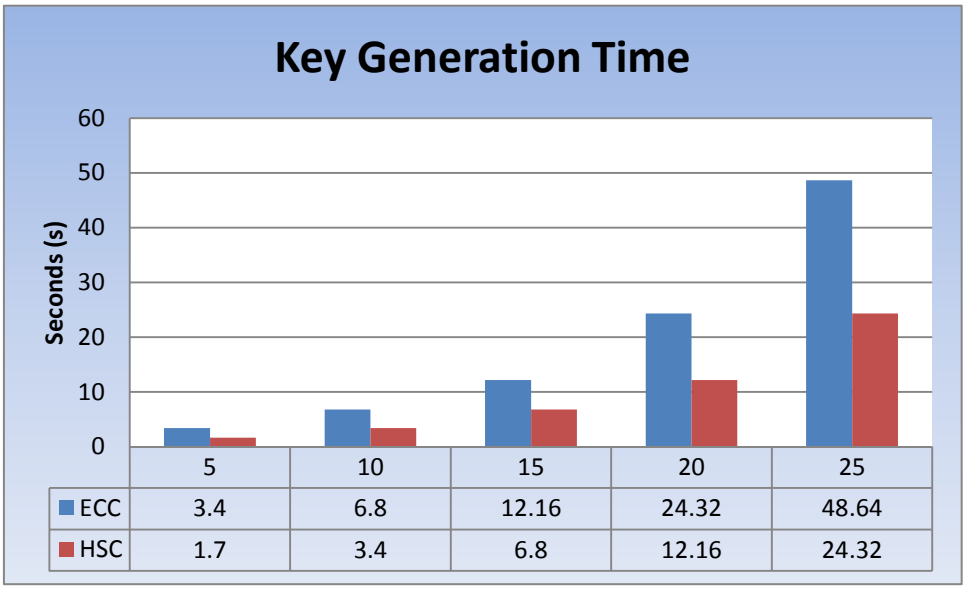


**Figure 6.** Key Generation Time

Table 5 shows the KGT for a varying number of SNs in the particular cluster for the proposed HSC protocol in comparison with the existing ECC protocol. The number of SNs in WSN for a particular cluster varying ranges from 5SNs to 25SNs. The results in Table 5 and Figure 6 show us that the KGT (seconds) of the proposed HSC protocol is significantly lesser by the increasing SNs than compare with the existing ECC protocol.

## 5. Conclusion

In recent times secure and energy-efficient data aggregation gained a lot of attention from researchers. In hopes of extending the service life of SNs, this work concentrated on strengthening their security and lowering their energy needs. According to the findings from the survey, numerous experts in the field of WSNs have used SN clustering as a method to cut down on network energy consumption. This research work focused on developing an alternative computational approach based on novel lightweight HSC protocol authentication which incorporates a pair-wise key establishment policy to establish energy-efficient data communication in large-scale WSNs. It adopts an authentication schema while performing pair-wise key management setup and also authenticates every SN belonging to an individual cluster before performing the data aggregation process. The experimental analysis shows the effectiveness of the proposed HSC protocol in terms of performance metrics is better than the existing ECC protocol. It also ensures an equilibrium between energy consumption and security requirements to enhance its adaptability to futuristic wireless applications. The goal of future research should be to develop secure protocols for mobile WSN networks that make the most efficient use of available power.

## References

[1] D. Liao, G. Sun, H. Li, H. Yu, and V. Chang, "The framework and algorithm for preserving user trajectory while using location-based services in IoT-cloud systems," Cluster Comput., vol. 20, no. 3, pp. 2283-2297, 2017, doi: 10.1007/s10586-017-0986-1.

[2] O. P. Yadav, "Internet of Things (IoT) security issue in wireless sensor network (WSN) with radio frequency identication (RFID)," SSSUTMS, Madhya Pradesh, India, Tech. Rep. 1, 2018.

[3] N. A. El-mawla, M. Badawy, and H. Arafat, "Security and key management challenges over WSN (a Survey)," Int. J. Comput. Sci. Eng. Surv. (IJCSES), vol. 10, no. 1, pp. 15-34, 2019.

[4] A. S. Naik and R. Murugan, "Security attacks and energy efficiency in wireless sensor networks: A survey," Int. J. Appl. Eng. Res., vol. 13, no. 1, pp. 107-112, 2018.

[5] S. B. Hassanpour, A. Diyanat, A. Khonsari, S. P. Shariatpanahi, and A. Dadlani, "Context-aware privacy preservation in network caching: An information theoretic approach," IEEE Commun. Lett., vol. 25, no. 1, pp. 54-58, Jan. 2021, doi: 10.1109/LCOMM.2020.3021919.

[6] T. Vaiyapuri, V. S. Parvathy, V. Manikandan, N. Krishnaraj, D. Gupta, and K. Shankar, "A novel hybrid optimization for cluster-based routing protocol in information-centric wireless sensor networks for IoT based mobile edge computing," Wireless Pers. Commun., pp. 1–24, Jan. 2021, doi: 10.1007/S11277-021-08088-W.

[7] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, "Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review," J. Netw. Comput. Appl., vol. 190, Sep. 2021, Art. no. 103118.

[8] H. Q. Qadori, Z. A. Zukarnain, M. A. Alrshah, Z. M. Hanapi, and S. Subramaniam, "CMIP: Clone mobile-agent itinerary planning approach for enhancing event-to-sink throughput in wireless sensor networks," IEEE Access, vol. 6, pp. 71464-71473, 2018.

[9] L. C. Mutalemwa and S. Shin, "Secure routing protocols for source node privacy protection in multi-hop communication wireless networks," Energies, vol. 13, no. 2, p. 292, Jan. 2020, doi: 10.3390/en13020292.

[10] Z. W. Hussien, D. S. Qawasmeh, and M. Shurman, "MSCLP: Multi-sinks cluster-based location privacy protection scheme in WSNs for IoT," in Proc. 32nd Int. Conf. Microelectron. (ICM), Aqaba, Jordan, Dec. 2020, pp. 1-4, doi: 10.1109/ICM50269.2020.9331785.

[11] G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, "A source location protection protocol based on dynamic routing in WSNs for the social Internet of Things," Future Gener. Comput. Syst., vol. 82, pp. 689-697, May 2018, doi: 10.1016/j.future.2017.08.044.

[12] B. Chakraborty, S. Verma, and K. P. Singh, "Differentially private location privacy preservation in wireless sensor networks," Wireless Pers. Commun., vol. 104, pp. 387-406, Jan. 2019, doi: 10.1007/s11277-018-6026-5.

[13] M. V. Babu, J. A. Alzubi, R. Sekaran, R. Patan, M. Ramachandran, and D. Gupta, "An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network," Mobile Netw. Appl., vol. 26, no. 3, pp. 1059–1067, Jun. 2021, doi: 10.1007/S11036-020-01664-7.

[14] Y. Wang, F. Li, P. Ren, S. Yu, and Y. Sun, "A secure aggregation routing protocol with authentication and energy conservation," Trans. Emerg. Telecommun. Technol., vol. 33, no. 1, Jan. 2022, Art. no. e4387, doi: 10.1002/ETT.4387.

[15] C. Pedroso and A. Santos, "Dissemination control in dynamic data clustering for dense IIoT against false data injection attack," Int. J. Netw. Manag., vol. 32, no. 5, May 2022, Art. no. e2201, doi: 10.1002/NEM.2201.