International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

Wireless Sensor Networks: A Hybrid Eecc-Eml Protocol for Improved Security and Energy-Efficiency

G. Viswanathan,
Ph.D. Research Scholar, Department of Computer Science,
SNMV College of Arts and Science, Coimbatore, Tamilnadu, India.

Dr. M. Jayakumar,
Assistant Professor, Department of Information Technology,
SNMV College of Arts and Science, Coimbatore, Tamilnadu, India.

ABSTRACT

An important function of a "Message-Authenticator (MA)" in "Wireless Sensor Networks (WSN)" is to prevent the transmission of unauthorized or flawed messages to preserve the sensors' limited energy resources. Numerous approaches that offer integrity and authenticity checking for messages transmitted over WSN are currently presented. Still, with those approaches, the "Sensor Node (SN)" containing the shared key, which frequently gets dispersed by several SNs, is solely capable of verifying the veracity and quality of the message. If an invader captures even a single SN, they will possess the key. Furthermore, these approaches fail to perform in multicast connections, and computing security formulas necessitate a major energy consumption. This research proposes a new hybrid protocol called "Enhanced Elliptic Curve Cryptography-Energy Modelling Language (EECC-EML)" to address the issue of limited energy efficiency while maintaining adequate security. The key concept behind the EECC is that the transmitting SN must create a source anonymized MA with every "Message (m)" before it can be shared. To protect the confidentiality of unconditionally clustered SNs during data exchange in WSNs, this method employs a "Ring-Signature (RS)" in which each ring SN is required to determine a forgery signature for each of the other SNs within its "Ambiguity Set (AS)". The core concept of EML aims to increase the efficiency of WSNs by the use of intermediary SN authentication on each hop. The suggested EECC-EML protocol outperforms the current HSC and CCAP protocols in terms of "Security Ratio", "Energy Consumption Ratio", "Computation Time", and "Key Generation Time".

***Keywords:** WSN, Message-Authenticator, Security, Energy-Efficiency, Ring Signature*

1. INTRODUCTION

With an immersed and interlinked society, WSNs are a game-changing technical development. In this, a large number of tiny SNs with limited resources engage with one another to gather and share information about their local environment. Due to their capacity to work together, WSNs have been put to use in many different industries, including medical IT, automated manufacturing, and ecological surveillance and monitoring [1].

However, there are limits to SNs that are intrinsic to the design, which include restricted storage, connectivity, processing capacity, and resources for energy. Preserving the privacy and anonymity of data have the utmost importance because these constraints provide complex hurdles when it comes to exchanging communication inside a network [2].

Another thing is that SNs may be attacked in many different ways, such as "Physical-Tampering (PT)", "Data-Interception (DI)", "Node-Compromise (NC)", and "Denial-of-Service (DoS)" threats [3]. The threats mentioned are especially hazardous when dealing with distantly installed and unsupervised SNs.

As a way to interfere with the activities of networks, intruders might conduct PT threats by interfering with the functions of SNs to interfere with how they operate, acquire sensitive information, or deactivate them. Security vulnerabilities caused by DI threats might expose confidential details to illegal parties. The confidentiality of data may be exploited with NC threats, while connection to the network as well as accessibility can be disrupted in DoS threats [4].

Interactions between "Cluster-Head (CH)" and "Base-Station (BS)" SNs encompass the exchange of sensitive information, the protection of which is of the utmost importance. Complex cryptography computations are frequently employed by conventional security methods that are implemented in WSNs. Regrettably, such methods significantly reduce the efficacy of communication by straining the SNs with a heavy energy load [5].

Because SNs have inherent energy constraints, this kind of high usage might shorten the network's operating lifespan by draining the energy of SNs and causing them to shut down prematurely. Such inefficiencies in energy usage become particularly problematic for systems that operate in real-time due to the need for minimal latency when trying to make quick decisions [6].

Although they mediate among SNs and the wider network architecture, CHs are nonetheless susceptible to security flaws. Intentionally, exploited CHs could open the door to cyberattacks, which might lead to the release of gathered information. Data integrity and confidentiality are under serious threat due to such intrusions, highlighting the need for confidence in CHs as an essential component of secure networks [7].

The invention of security methods that minimize the consumption of energy is becoming an important focus in WSNs due to the growing importance of effective energy utilization. Modern methods, including compact encryption algorithms, need to be investigated to find a middle ground between the security of information and energy saving [8]. The adoption of centralized administration platforms is necessary to solve many problems, such as assurances, latency, and flexibility, while securely transferring information within SNs across distinct clusters [9].

Problem Statement: By using a semi-trusted gateway for decoding information before sending it from a single device to a different one, current security protocols make it possible to communicate and share information securely across a network despite revealing the contents or the keys. A reputable third-party provides a fresh encryption key which guarantees that the information stays secret and safe all over the whole transmission process, allowing this to be a flawless transition [10]. While current sophisticated protocols work well on big devices with plenty of resources, they aren't effective if implemented on small devices with limited resources, such as SNs. The present protocol's approach necessitates complicated cryptographic computations, which result in high processing expenses and therefore lower efficiency. Systems with restricted capacity for processing and resources for energy tend to be less suited to use such protocols due to the resource-expensive operations they need. Furthermore, the protocol's computing time grows in proportion to the growing amount of SNs involved in sharing information, and this effect increases the likelihood of delays during the re-encryption operation and, by implication, the general effectiveness of the network's operations along with the transmission of information instantaneously is getting lag.

Paper Contribution: This present research introduces a novel EECC-EML protocol designed to be employed with AS within WSNs, that overcomes those drawbacks. The newly developed protocol greatly improves the security of WSN interactions and exchanges of data by using portable forms of encryption. With the suggested EECC-EML protocol, ASs could more easily handle accumulated information over multi-hop communications across intermediate SNs over routing, thereby mitigating security concerns like NC and DI. To further guarantee ensuring no other SN associated with the AS can read or retrieve encrypted information, the suggested EECC-EML protocol adopts a constant encryption approach. Optimal consumption of energy and reduced latency when communicating are two other areas where it excels.

Paper Organization: Section 2 presents a review of the published literature on secure and energy-efficient information transfer across WSNs, Section 3 explores the methodologies that comprise the suggested EECC-EML protocol, Section 4 deals with comparing and contrasting the results obtained from implementing the current HSC, and CCAP protocols with those of the proposed EECC-EML protocol, and Section 5 concludes what was researched and gives suggestions for potential future scope.

2. RELATED WORKS

Within WSNs, the researchers of [11] suggested a "Query Privacy-Preserving for Data Aggregation (QPPDA)". The overall WSN has been split among many cells, forming a grid-oriented network architecture. The "Homomorphic-Encryption" method is used to secure the information collected by the cell's member SNs within the QPPDA, which gathers the information in response to the incoming query. The process continues with securely encrypted information transmitted by every single SN to the aggregating SN, which then aggregates the information collected from the SNs within its cell and delivers the information to the BS. Implementing the "Homomorphic-Encryption" approach, the key generating procedure within the QPPDA has a large computing cost and is unable to ensure the information's authenticity.

To protect WSNs across the IoT against DoS threats, the researchers of [12] suggested a robust DA protocol. The "Blowfish-Encryption," "EAX-mode," and "RSA" algorithms are used by this network protocol. With its DOS threat resistance and capacity to meet the frequently disregarded availability of data privacy criteria, it constitutes a formidable contender. Data aggregation, still involves two sets of decryption and encryption processes, thereby increasing the transmission strain on SN.

A protocol called the "Coverage-Optimization and Hole-Healing Protocol (CHHP)" has been developed for implementation in WSNs by the researchers [13]. Using sleeping and wake-up processes, the protocol had the objective of improving the coverage of networks and fixing covering holes. A notable 30% improvement in the coverage of networks and a successful reduction of insufficient coverage are shown by the experiment's findings.

The researchers of [14] presented an approach for WSN collecting data using an improved "Online-Sequential Extreme-Learning Machine (OSELM)" along with the "Gray-Wolf Optimization (GWO)" algorithm. The strategy's goal is to improve data-collecting efficiency by controlling the energy used for transmission associated with the Grouping Model's SNs in a flexible way. The results of the experiment show that, in comparison to the traditional methods, the data-collecting effectiveness is 25% higher.

A WSN clustering and "Sleep-Scheduling" technique based on "Particle-Swarm Optimization (PSO)" was presented by the researchers in [15]. This technique aimed to improve the efficiency of energy through forming efficient clustering and automatically determining sleeping and wake-up periods for SNs. A notable 50% drop in consumption of energy and a substantial 60% improvement in network lifespan is shown by the experiment's findings.

3. METHODOLOGIES

This research aims to address the subsequent risks to WSN instantaneous interaction in context with the information privacy problems. There are primarily two kinds of attacks:

Passive-Attacks: The attackers in these assaults might examine network activity and eavesdrop on messages in transit.

Active-Attacks: These attacks can commence from SNs that have been exposed. Whenever rivals gain access to the SNs, they will be able to access any data contained in them, which might involve the security settings. Rivals can alter the message material and insert their desired instructions.

Technologies for exchanging data and voice through WSN are expanding at a fast pace. Because of these advancements, their examination and assessment of performance are now necessary. Efficiency in energy use has been one of the primary areas of research into WSN deployments. Furthermore, it is important to speculate about how to strike a balance between energy efficiency and security. For the system to meet the necessary performance standards, it is crucial to develop confidential protocols.

3.1 HSC PROTOCOL

A mechanism called "Hashing Signature Code (HSC)" has been presented in [16] to solve the problems with traditional WSN security by balancing the competing needs for effective exchange of information and minimal resource use. An HSC protocol with a "Pairing keys (PK)" formulation procedure is used to verify SNs. The envisioned HSC architecture makes utilization of a confidential shared-key element, the application of which is restricted to the SiN and SNs. Building a PK with two separate SNs eliminates the need for a certificate-based authorization method. In each particular cluster, every SN uses the same unique identification. An authorization system that is both secure and resistant to cloned and imposter assaults is part of the HSC security modeling. Using a predetermined sequence of participating categories, the above-mentioned framework is designed to work systematically by constructing clusters of SNs, and then by aggregating all the data coming from "Member Nodes (MNs)" inside these clusters. The employment of the hashing technique for verifying communications using the process of aggregation is crucial to both authorization privacy and information integrity. By combining every one of the communication processes into a single stage, hashing eventually accomplishes cryptography and key validation. Concerning its effective authenticating mechanism, this particular version is specially designed to be immune to "Cloning and Impersonation Attacks".

3.2 CCAP PROTOCOL

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

For WSN transmitting information alongside the greatest precision and reduced energy consumption, a CCAP protocol has been suggested in [17] to solve the related challenge of defining the issue and extracting an outstanding performance, optimized solution. The suggested CCAP protocol uses graph-based transmission to construct a WSN system at the outset of the communication operation. The suggested system uses group-based interactions among SNs and CHs, as well as amongst CHs and SiN after the initial interaction takes place among SNs with the exchange of control signals. Moreover, the suggested CCAP protocol encodes control signals and information to be transferred from origin to target SN inside a WSN using an encrypted approach, while simultaneously using modest energy. While the encryption keys have been utilized to decipher the control signals that have been routed, there is a risk that the ciphered information might end up in an unauthorized SN due to the way it is generated. However, the information will be difficult for the attacker to decipher since the procedure is not repetitive and relies on several cryptographic assumptions. Given that it uses multipart schemes for encryption to decode data, it effectively blocks intruders from engaging in any illegal activities. Here, the intruder has to keep going for as extended as possible to raise the odds of being captured.

3.3 EECC-EML PROTOCOL

3.3.1 EECC

The EECC proposed in this research is both an effective and completely secure method. An unidentified source MA has been generated by the message the transmitter, also known as the transmitting SN, before every "message (m)" gets published. Crucial inside this generating process are the ECs. Every ring SN within an AS has to have its "forgery signature" estimated for each of the other ring SNs for there to be an RS. The "Ring-Structure" idea is used in this present research to ensure the confidentiality of unconditionally anonymized SNs during data exchange within WSNs.

(i) Building a "Ring-Structure" involves the following phases:

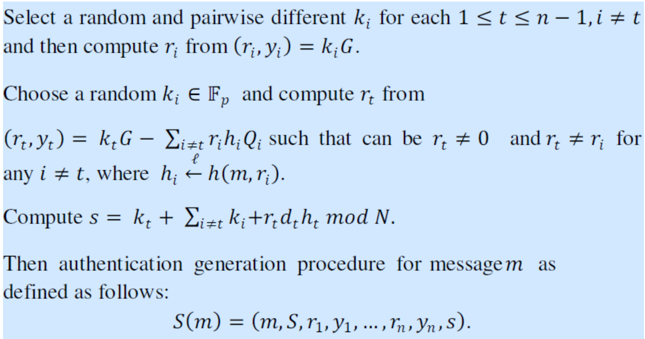
- To ensure accurate verification, RSs have been developed in a manner that the ring is capable of being "completed" using confidential data, usually a "Private-Key (PrK)" that corresponds to a particular "Public-Keys (PuK)" inside the ring.
- Every PuK within the ring gets assigned a number that is chosen at random during the "Signature-Generation" process. The SN which signs then utilizes its own PrK information or similar "trapdoor information" for closing the ring.
- By encapsulating SN operations in a larger set of operations, RSs provide SNs with a measure of privacy. Having excellent availability means that operations could happen fast as well and operations are capable of being successfully combined, having significant resistance to planned amalgamating analytical threats. This is achieved when several SNs contribute relatively comparable values to the ring.
- It employs 64-bit header construction for transferring messages to carry out this technique in data transfer.
- With this scenario, there are only 3 stages to generate an EECC, and they connect the data transmitter and all non-transmitters to it. Furthermore, the SNs may be validated using one equation according to this architecture, saving time compared to independently confirming each signature.

For contention, let's presume that SN (A) is prepared to secretly send a "m" for any SN. Concerning a certain "Value (t), $1 \leq t \leq n$", the AS comprises "Members (n) [A_1, A_2 … …, A_n]", including "S = [A_1, A_2 … …, A_n]", whereas the original originator SN was "A_t". Here, it doesn't distinguish between the "SN (A_i)" as well as their "PuK (Q_i)". This means that it additionally has "S = [Q1, Q2, ….., Qn]".

(ii) Mechanism for Authentication-Generation:

Consider that "m" is being sent. The message "A is dt , $1 \leq t \leq N$" has a PrK of SN. The EECC method's authentication-generating approach is shown in Algorithm 1. Below are the 3 stages that SN "A" takes to produce a successful EECC over "m":

Algorithm 1: EECC



Select a random and pairwise different k_i for each $1 \leq t \leq n-1, i \neq t$ and then compute r_i from $(r_i, y_i) = k_i G$.

Choose a random $k_i \in \mathbb{F}_p$ and compute r_t from

$(r_t, y_t) = k_t G - \sum_{i \neq t} r_i h_i Q_i$ such that can be $r_t \neq 0$ and $r_t \neq r_i$ for any $i \neq t$, where $h_i \overset{\ell}{\leftarrow} h(m, r_i)$.

Compute $s = k_t + \sum_{i \neq t} k_i + r_t d_t h_t \ mod \ N$.

Then authentication generation procedure for message m as defined as follows:

$$S(m) = (m, S, r_1, y_1, \dots, r_n, y_n, s).$$

***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

(iii) *Security Analysis over EECC*

Here, it examines the evidence that the suggested EECC can protect messages from certain types of attacks while simultaneously providing uncompromising source anonymity and proving that they can't be altered.

(a) Anonymity: The suggested EECC technique provides absolute security for the message's transmitter SN's identity. That's because for any given transmitter SN, it has precisely "(N − 1), (N − 2), … (N − n)" distinct ways to produce the EECC. No complexity-theoretic hypotheses are required for most of them to be chosen out of any AS's SN as part of the EECC-generating method with comparable probability. There is clear proof confirming the additional attribute, which states this EECC may be generated by whatever SN from origin S.

(b) Unforgeability: Considering certain message assaults according to the "Random Oracle" paradigm, the suggested EECC is protected towards existential forging.

Choice of AS and Source Confidentiality: To ensure information origin privacy, it is crucial to choose the right AS, because it will conceal the real SN that is sending the message. The considerations that follow may be used to define the AS selection process:

- To make it possible for the message's origin SN to maintain source-to-destination privacy, it must choose an AS that allows SNs originating in every direction to be included. Specifically, the AS has to incorporate SNs that are in the opposing path of the succeeding SN.
- Here, neither every next-in-line SN won't be competent to tell the difference between the sender and the receiver of the message. Although any of the SN within the AS could be chosen by the message's origin SN, also those SNs can't provide uncertainty to the message's origin SN. As a result, according to geographical routing, it seems to be impractical for the inclusion of SNs within the AS. Due to this, the AS doesn't need to consider these SNs. For the sake of energy efficiency, they shouldn't be part of the AS.
- It attempts to choose SNs that are around a certain distance limit relative to the routing path to strike a compromise between source confidentiality and performance. Among the SNs within a band that encompasses the current routing path, it suggests picking an AS. Nevertheless, not every SN has to be included within the routing path by the AS.
- The AS doesn't need to incorporate every SN within the specified range or along the current routing path. In reality, an attacker could potentially be able to determine the origin SN and probable routing paths when every SN exists within the AS.

3.3.2 EML

Among the main functions of the EML function was to assess the system's "Energy Consumption (EC)". The EC of a system is determined by adding up the energy used by the radio waves of a single SN and the energy used by basic processes that rely solely on the "Central Processing Unit (CPU)", the CPU's processes are security procedures, mathematical calculations, and so on. Equation (1) shows how the EC of a single SN's communications activity or CPU is determined:

$$E_{op} = T * I * V \qquad \text{Eq}\rightarrow 1$$

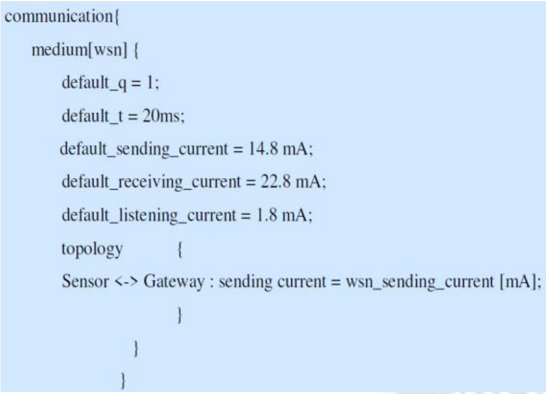
From Equation (1) the notions are "Operation's Time is (T)", "Operations Electric-Current is (I)", "SN or Host's Voltage is (V)", and "CPU's EC is (E_{op})". The EML assessment concludes by doing the following evaluations of the EC for every host and SN as per Equation (2):

$$E_H = E_{H_{CPU}} + E_{H_{COMM}} \qquad \text{Eq}\rightarrow 2$$

From Equation (2) the notions are "SN/ Host's EC (E_H)", a "Total EC for every CPU's Operation (E_{HCPU})", a "Total EC for all Sending, Receiving, and Listening Communication Operations (E_{HCOMM})".

The 3 new variables "Sending-Current (SC)", "Receiving-Current (RC)", and "Listening-Current (LC)" is introduced by the EML function. They all provide 3 separate descriptions of the "Electric-Current (ELC)" in terms of states. Whenever a host or SN awaits expecting a message over the channel, the ELC is defined by the LC. Since hosts and SNs may transmit and acquire information with varying ELCs (e.g., the SC for sensors may fluctuate based on the signal's intensity), the ELC within the mode of transmission was split into 2 parts: the SC and the RC. Algorithm 2 demonstrates the EML methods' Communications activities alongside a CPU utilization methodology which is predictable.

Algorithm 2: EML



```
communication{
   medium[wsn] {
        default_q = 1;
        default_t = 20ms;
        default_sending_current = 14.8 mA;
        default_receiving_current = 22.8 mA;
        default_listening_current = 1.8 mA;
        topology        {
        Sensor <-> Gateway : sending current = wsn_sending_current [mA];
                         }
                   }
                 }
```

The following Equation (3) is the description of the "Life Time of Nodal is nl(G,v)" from SN (V) within the WSN system symbolized by "Graph (G)":

$$nl(G,v) = \frac{E_r(v)}{E_{CPU}(v) + E_{COMM}(v)}$$ Eq→3

From Equation (3) the notions are "SN (v)'s Residual-Energy is (E_r(v))", "Overall CPUs Energy is (E_{CPU}(v))", and "SN (v)'s Communication-Functions is (E_{COMM}(v))". In this context, "Overall CPU's activities" was defined in the following Equation (4):

$$E_{CPU}(v) = \sum_{i=CPU} E_i(v)$$ Eq→4

Each CPU activity is defined with its own EC and "CPU" is a collection of indices for all CPU activities. Equation (5) defines how every communication activities are outlined:

$$E_{COMM}(v) = \sum_{i=COMM} E_i(v)$$ Eq→5

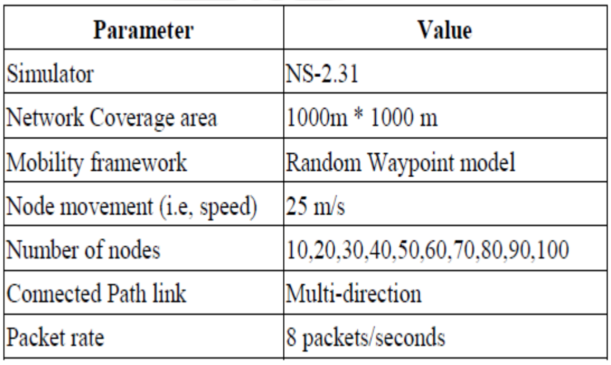
Whereas the "COMM" refers to the set of "Sending, Receiving, and Listening" communication activities indices. Thus the suggested EECC-EML protocol achieves the balance between security and energy-efficiency by choosing the best energy-efficient variant that delivers the necessary degree of security in a certain amount of time.

Advantages: This suggested EECC-EML protocol strikes a balance between the two competing goals of data privacy as well as efficiency. Furthermore, models for dealing with situations requiring increased effectiveness or security may be developed using this research. For instance, a sharp shift in the weather might signal a heightened need for efficiency, which is an unforeseen and substantial change in environmental parameters. Conversely, heightened security measures might be implemented in response to the identification of unusual communication.

4. RESULTS AND DISCUSSIONS

The current HSC, CCAP, and developed EECC-EML protocols were all successfully implemented in a simulated military environment using the "NS-2 Simulator," which has networking sizes of "1000m*1000m". A secured site had been designated for the WSN's SN to monitor environmentally related work and detect "Military Data (MD)" trails. A sampling duration of "25 milliseconds" was determined and used for various operations. Any SN inside the system has become autonomous to choose any route that is accessible according to the "Random Way Point (RWP)" concept. When RWP is setting up a network, it often employs the median number of SNs. Table 1 provides the settings needed for running the simulations and performing the experiments. The modeling findings are obtained by performing several repeated runs across multiple setups. This research project compares the current HSC and CCAP protocols with the new EECC-EML protocols to determine which one is more effective. Visual tools like tables and graphs allow for the evaluation of efficiency comparisons with pinpoint accuracy.

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):

The SR associated with an MD is determined by the percentage of its information which was transmitted successfully relative to the whole volume of information. Equation (6) has been employed to quantitatively establish the SR, which is often characterized as "Percentage (%)" that was found by analyzing MD records. The approach is considered effective while MD exhibits a superior SR.

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

Eq→6

Table 2: Security Ratio

Average Military Data	HSC	CCAP	EECC-EML
100	95	97	99
200	92	94	96
300	89	91	93
400	86	88	90
500	83	85	87

Table 2 shows the results of comparing the suggested EECC-EML protocol against the current HSC and CCAP protocols for different SNs MD using the SR measurement. Inside the WSN, MD readings ranging from 100 to 500 were collected and logged. The EECC-EML protocol outperforms the current HSC and CCAP protocols in terms of SR of MD, as shown in Table 2 and Figure 1. The suggested EECC-EML protocol enhances the SR associated with the MD records, as shown by comparing its SR with that of the current HSC and CCAP protocols, each of which includes 500 records.

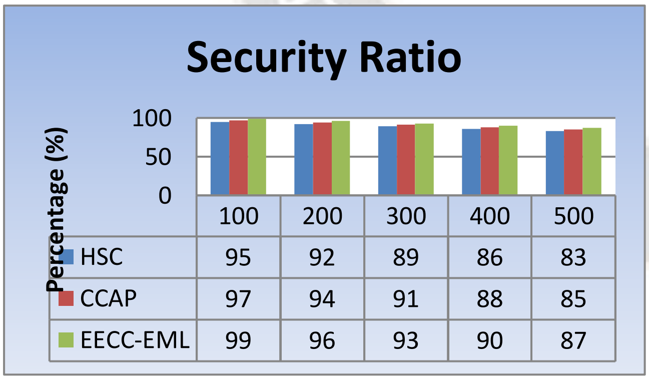


Figure 1:Security Ratio

(ii) Energy-Consumption Ratio (ECR):

Through evaluating the energy consumption of one SN with the total across all SNs inside a WSN, the suggested EECC-EML protocol measures the ECR for MD transmission among SNs. It is possible to transform the ECR towards "Joules (J)" by using the following Equation (7):

$$\text{Energy Consumption Ratio (ECR)} = \text{Individual SN Energy} * \text{Total SNs Energy}$$

Eq→7

Energy with a particular SN "EnergySN", multiplied with the overall number of SNs across WSN networks "TotalSN," gives the ECR for reliable remote MD operations. The protocol that was implemented was found to be effective when the ECR was minimal.

Table 3 shows the ECR for different military SNs, and demonstrates how the suggested EECC-EML protocol compares to the current HSC and CCAP protocols. Within WSN, the SN level could range from 20 to 100. Table 3 and Figure 2 demonstrate that compared against the established HSC and CCAP protocols, the EECC-EML protocol reduces the ECR for SN. Observations have shown that ECR varies between protocols within the range of 180 to 3900 joules. The current HSC and CCAP protocols consume "3900 J" and "3600 J" of energy during secured management of the MDs, whereas the suggested EECC-EML protocol consumes "3300 J" considering SN constitutes 100. Compared to the current HSC and CCAP protocols, the suggested EECC-EML protocol results in a reduced ECR. Figure 2 is a visual depiction of the data presented in Table 3.

Table 3: Energy Consumption Ratio

Total SNs	HSC	CCAP	EECC-EML
20	780	480	180
40	1560	1260	960
60	2340	2040	1740
80	3120	2820	2520
100	3900	3600	3300

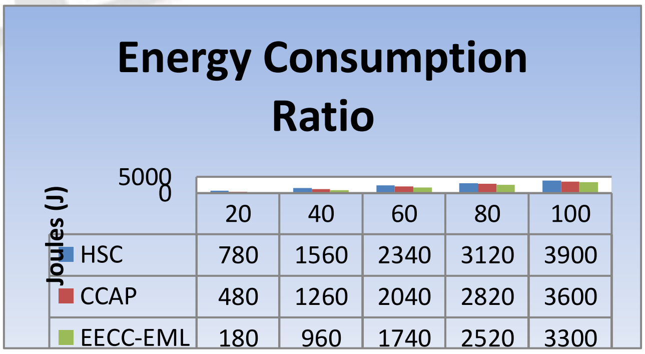


Figure 2: Energy Consumption Ratio

(iii) Computation Time (CT):

From any anticipated sizes of the MD, the CT determines the duration and capacity needed for the operation to be performed. It is possible to predict the memory demand (the number of storage regions) or the pace of converging (the absolute magnitude of operations) for various protocols from the dimension of the input, as indicated in Equation (8):

$$\text{Computation Time} = \text{Amount of time for computing}$$

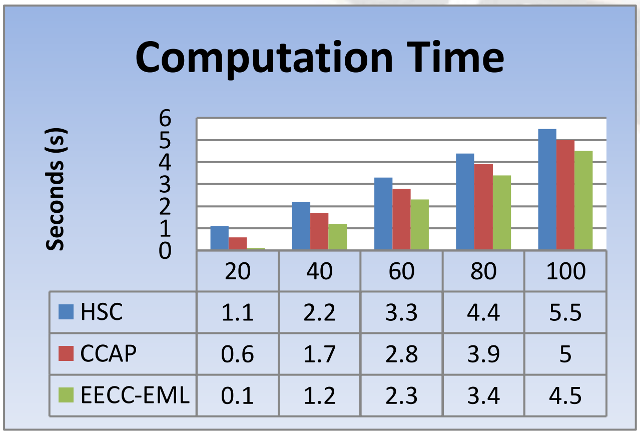
Eq→8

A well-executed protocol will result in outcomes using this metric which are likely minimal or increase steadily as it gets larger MD sizes.

The CT for different SN's MD values utilizing the current HSC, CCAP, and the suggested EECC-EML protocols have been compared in Table 4. The maximum and minimum sizes for SNs MD records within WSN are "20 KB" and "100 KB" respectively. Table 4 and Figure 3 show that the suggested EECC-EML protocol's "Computational Time (Seconds)" lowers at a considerably quicker pace as the "Data Size (KB)" grows compared to the current HSC and CCAP protocols.

Table 4: Computation Time

DataSize (KB)	HSC	CCAP	EECC-EML
20	1.1	0.6	0.1
40	2.2	1.7	1.2
60	3.3	2.8	2.3
80	4.4	3.9	3.4
100	5.5	5	4.5



	20	40	60	80	100
🟦 HSC	1.1	2.2	3.3	4.4	5.5
🟥 CCAP	0.6	1.7	2.8	3.9	5
🟩 EECC-EML	0.1	1.2	2.3	3.4	4.5

Figure 3: Computation Time

(iv) Key Generation Time (KGT):

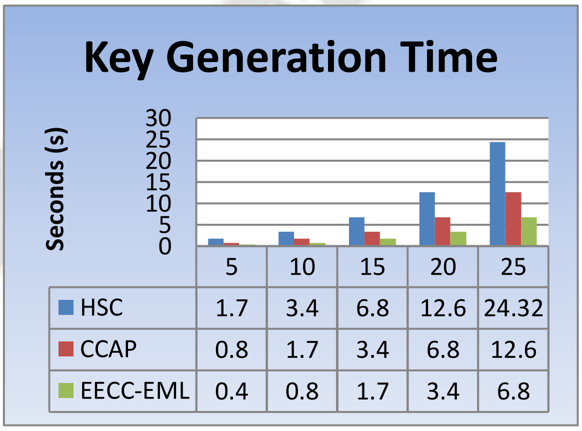
While "N-1 SNs leaves" or "Join New Cluster" or AS occurs, the process of upgrading the "Cluster-Key" is called KGT. "Cluster-Key" modifications will be considered less often by the CH if "N-l SNs Leave or Join any Cluster" for a long time. Given the intricacy of the current HSC and CCAP protocols, the proposed EECC-EML protocol streamlines the process of creating an encryption key, making it less tedious and ultimately more effective. Therefore, the system's responsiveness is due entirely to its lightweight and portable construction. Once the total number of SNs within a certain cluster is updated, the KGT may be calculated in a single computation following Equation (9):

$$\text{Key Generation Time} = \frac{\text{Cluster Key Generation}}{\text{Join / Leave Clusters}}$$

Eq→9

Table 5: Key Generation Time

Number of SNs	HSC	CCAP	EECC-EML
5	1.7	0.8	0.4
10	3.4	1.7	0.8
15	6.8	3.4	1.7
20	12.6	6.8	3.4
25	24.32	12.6	6.8



	5	10	15	20	25
🟦 HSC	1.7	3.4	6.8	12.6	24.32
🟥 CCAP	0.8	1.7	3.4	6.8	12.6
🟩 EECC-EML	0.4	0.8	1.7	3.4	6.8

Figure 5: Key Generation Time

Across an array of cluster dimensions and SN counts, Table 5 compared the KGT for the suggested EECC-EML protocol against those current HSC and CCAP protocols. Depending on the cluster, WSNs may include ranging from 5 to 25 SNs. The suggested EECC-EML protocol features a firmly reduced KGT (seconds) for increasing SNs compared to the current HSC and CCAP protocols, as shown in Table 5 and Figure 4.

5. CONCLUSIONS

To provide hop-by-hop MA without the weakness of the built-in threshold, this research proposed an EECC-EML protocol to address the issue of limited energy efficiency while maintaining adequate security. The key concept behind the EECC is that the transmitting SN must create a source anonymized MA with every message before it can be shared. The core concept of EML aims to increase the efficiency of WSNs by the use of intermediary SN authentication on each hop. Finally, the extensive numerical analysis demonstrated that the proposed EECC-EML protocol attains better communication performance and energy efficiency regardless of having any major dependency on computational resources while implemented as compared to the existing HSC, and CCAP protocols. The proposed EECC-EML protocol exhibits robustness against active and passive WSN threats, such as "Replay-Attack", "Sybil-Attack", "Man-in-the-Middle Attack", "Brute-Force Attack", etc. Addressing real-world implementation circumstances and studying the protocol's adaptability and efficiency in certain WSN contexts will be part of future investigations aimed at making the suggested EECC-EML protocol more applicable to resource-constrained WSNs.

REFERENCES:

[1]. O. A. Khashan, R. Ahmad, and N. M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," Ad Hoc Networks, vol. 115, p. 102448, 2021.

[2]. O. A. Khashan, S. Alamri, W. Alomoush, M. K. Alsmadi, S. Atawneh, and U. Mir, "Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments," Computers, Materials & Continua, vol. 75, no. 2, 2023.

[3]. I. Mashal, O. A. Khashan, M. Hijjawi, and M. Alshinwan, "The determinants of reliable smart grid from experts' perspective," Energy Informatics, vol. 6, no. 1, pp. 1-23, 2023.

[4]. O. A. Khashan and N. M. Khafajah, "Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems," Journal of King Saud University-Computer and Information Sciences, vol. 35, no. 2, pp. 726-739, 2023.

[5]. A. Sufyan, K. B. Khan, O. A. Khashan, T. Mir, and U. Mir, "From 5G to beyond 5G: A Comprehensive Survey of Wireless Network Evolution, Challenges, and Promising Technologies," Electronics, vol. 12, no. 10, p. 2200, 2023.

[6]. F. H. El-Fouly, M. Kachout, Y. Alharbi, J. S. Alshudukhi, A. Alanazi, and R. A. Ramadan, "Environment-Aware Energy Efficient and Reliable Routing in Real-Time Multi-Sink Wireless Sensor Networks for Smart Cities Applications," Applied Sciences, vol. 13, no. 1, p. 605, 2023.

[7]. Z. A. Zukarnain, O. A. Amodu, C. Wenting, and U. A. Bukar, "A survey of Sybil attack countermeasures in underwater sensor and acoustic networks," IEEE Access, 2023.

[8]. O. A. Khashan, N. M. Khafajah, W. Alomoush, M. Alshinwan, S. Alamri, S. Atawneh, and M. K. Alsmadi, "Dynamic Multimedia Encryption Using a Parallel File System Based on Multi-Core Processors," Cryptography, vol. 7, no. 1, p. 12, 2023.

[9]. K. Jain, P. S. Mehra, A. K. Dwivedi, and A. Agarwal, "SCADA: scalable cluster-based data aggregation technique for improving network lifetime of wireless sensor networks," The Journal of Supercomputing, vol. 78, no. 11, pp. 13624-13652, 2022.

[10]. O. A. Khashan, "Parallel proxy re-encryption workload distribution for efficient big data sharing in cloud computing," in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 554-559.

[11]. Liu X, Zhang X, Yu J, Fu C (2020) Query privacy preserving for data aggregation in wireless sensor networks. Wirel Commun Mob Comput 2020:1–10.

[12]. Dener M (2022) SDA-RDOS: A New Secure Data Aggregation Protocol for Wireless Sensor Networks in IoT Resistant to DOS Attacks. Electronics 11(24):1–30.

[13]. V. Narayan, A.K. Daniel, CHHP: coverage optimization and hole healing protocol using sleep and wake-up concept for wireless sensor network, Int. J. Syst. Assur. Eng. Manag. 13 (Suppl 1) (2022) 546–556.

[14]. Y. Bai, L.i. Cao, S. Wang, H. Ding, Y. Yue, L. Xu, Data collection strategy based on OSELM and gray wolf optimization algorithm for wireless sensor networks, Comput. Intell. Neurosci. 2022 (2022) 1–18.

[15]. P. Rawat, S. Chauhan, Particle swarm optimization-based sleep scheduling and clustering protocol in a wireless sensor network, Peer-to-Peer Network. Applicat. 15 (3) (2022) 1417–1436.

[16]. G. Viswanathan, and Dr. M. Jayakumar, (2023). A Novel Authentication Protocol for Wireless Sensor

Networks to Enhance Security with Energy-Efficiency. European Chemical Bulletin, 12(Si6), 5828–5850. https://doi.org/10.48047/ecb/2023.

[17]. G. Viswanathan and M. Jayakumar, "A Novel CCAP Protocol to Increase Security with Energy Efficiency for Wireless Sensor Networks," 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2023, pp. 1689-1697, doi: 10.1109/ICECA58529.2023.10395236.