Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

DSGARS: SYMBOLICDELTAALPHANUMERIC-BASED SECURE AND ANONYMOUS ROUTING IN WIRELESS SENSOR NETWORKS

Mr. A. PradeepKumar,Research Scholar (PT), Department of Computer Science, Defence Institute of Advanced Technology, Pune - 411 025Assistant Professor, Department of Computer Science,S.V.N College -Madurai-625 019.
Dr. Dinesh Senduraja Ph.D. Research Associate (RA), MED& COS, Defence Research & Development Organisation (DRDO) Pune- 411 021.
Lecturer, Government Art and Science College, Veerapandi, Theni -625 534.
Dr.V. IsakkirajanPh.D, Assistant Professor (HOD), Department of Computer Science, P.K.N Arts & Science College -Tirumangalam-625 706.

ABSTRACT:
In recent years, considerable research has focused on energy efficiency and security in wireless sensor networks (WSNs). However, few studies have successfully identified a routing method that is secure, cost-effective, and energy-efficient. This research aims to ensure energy-efficient routing in WSNs by utilizing public key cryptography. The proposed work introduces a method called DSGARS (Delta-Alphanumeric Sign-Based Secured Anonymous Routing in Wireless Sensor Networks), which authenticates the routing data exchanged between sensors. DSGARS ensures the verification of all participating nodes within the network and leverages oblique curve cryptanalysis as the foundation for security protocols. Through an innovative sign-based approach to public key encryption, the system adds an extra layer of security.
The findings of the study reveal that DSGARS surpasses other security-focused and energy-efficient routing protocols in terms of both performance and effectiveness. DSGARS introduces a comprehensive framework that integrates three innovative components. The first component is an alphanumeric sign scheme, which ensures secure routing by using unique alphanumeric identifiers to authenticate nodes and messages, reducing the risk of impersonation attacks. This mechanism strengthens the integrity of data exchange between nodes, ensuring that only legitimate nodes participate in the communication process.
The second component is a privacy or anonymity scheme, designed to protect the identities of nodes and their interactions within the network. By anonym zing the nodes, DSGARS minimizes the chances of adversaries tracking communication patterns, making it difficult for malicious actors to compromise specific nodes or interfere with data transmission.
The third component is an advanced public key encryption strategy, which adds a robust layer of security to data transmissions. By leveraging lightweight public key cryptography, DSGARS ensures that messages are securely encrypted before being transmitted across the network. This method not only maintains data confidentiality but also enhances energy efficiency by optimizing encryption processes to suit the constrained resources of sensor nodes.
The results demonstrate that DSGARS delivers superior performance when compared to widely used protocols such as SLEACH, LEACH, and PSDCSIS. Unlike these existing protocols, which often focus on either energy efficiency or security, DSGARS achieves a balanced optimization of both. It minimizes energy consumption without compromising security, making it well-suited for real-time, resource-constrained wireless sensor networks. The combination of these three novel components allows DSGARS to provide a more resilient, cost-effective, and reliable routing solution, ensuring enhanced network longevity and data protection.

Keywords: *SLEACH, LEACH, PSDCSIS*

INTRODUCTION:

Wireless sensor networks (WSNs) are primarily utilized in scenarios where human intervention is impractical, such as atomic plant monitoring, territorial surveillance, weather forecasting, and forest fire detection. In these applications, sensors are typically deployed from low-altitude aircraft with the primary objective of environmental monitoring, including tracking motion, temperature, heat, pressure, and smoke. Data aggregation is the process through which these sensors collect information and transmit it to the appropriate destination [1,2].

However, sensors face limitations such as low computational capacity, limited processing power, and small buffer sizes. Before transmitting individual data to the next cluster head and eventually to the base station, the data undergoes a fusion process that eliminates redundancies using a voting system and specific statistical methods. This processed data is highly valuable and can attract unauthorized access by adversaries. In a WSN, an enemy node may either infiltrate the network after the sensors are deployed or already exist within the monitored area.

A deeper analysis of the literature reveals that extensive research has been conducted on addressing the challenges of energy efficiency and security.Routing protocols play a crucial role in sensor networks [3]. Before transmitting data to the next cluster head (CH) and ultimately to the intended destination, the data must first pass through a fusion process that eliminates redundancies using a voting mechanism and specific statistical methods. This processed data holds significant value and is often targeted by unauthorized entities, referred to as adversaries. An enemy node can either infiltrate the network post-deployment or may already exist within the monitored area. A detailed review of the literature reveals that extensive research has been conducted on energy efficiency and routing protocols in sensor networks [4].

Since sensor networks rely on remote access policies, they are particularly vulnerable to privacy breaches. However, due to the limited computational capacity of sensor nodes, advanced cryptographic protocols cannot be directly implemented. Effective cryptographic methods must ensure non-repudiation, confidentiality, privacy, integrity, and authentication, all while maintaining efficiency. Consequently, most researchers in the field of security systems have focused more on routing-based methods rather than node-based systems. While node-based cryptographic techniques struggle to provide long-term security, routing-based approaches require active maintenance to store and apply the required management protocols [5].

Therefore, a reliable and cost-effective authentication mechanism is essential. Public key cryptography has emerged as the most efficient and lightweight encryption solution. However, the keys generated through this process are still vulnerable because they must be shared with the target node. The use of oblique curve cryptography has shown promise in providing secure encryption, but its long-term durability and economic feasibility in WSNs remain under scrutiny.

This study proposes a robust authentication mechanism between nodes, striking a balance between energy efficiency and security resilience by implementing a low-cost public key encryption scheme. It introduces a novel public key cryptography system along with a unique sign-based technique to address existing security challenges. After reviewing previous security techniques in Section 2, Section 3 outlines the identified challenges. Section 4 presents an overview of the proposed system, followed by a detailed discussion of the research process in Section 5. The algorithms are explored in Section 6, and the results are analyzed in Section 7. Finally, the paper is concluded in Section 8.

RELATED WORK:

This section covers research conducted on secure communication in wireless sensor networks (WSNs). Most studies in [6] have provided recommendations to enhance encryption key management in WSNs. The authors also employed hashing techniques to minimize latency. It was revealed that energy efficiency could be achieved by using MD5 encryption. However, the authors did not compare their results with any existing solutions. In [7], an encryption method was presented that combines evolutionary algorithms with chaotic maps. The authors verified the authenticity of active sensors using public key cryptography (such as oblique curve cryptography). Experiments with real sensors demonstrated whether the proposed method outperformed advanced block cipher algorithms. Notably, the authors assessed the technique's effectiveness through entropy, CPU cycles, and memory consumption, using image data.

An overview of cryptographic approaches utilizing optimization techniques in WSNs are provided in [8], while [9] discusses communication security in heterogeneous sensor networks. Their study also addressed energy consumption challenges and proposed a key exchange framework to enhance security. In [10], the focus was on accelerating public key encryption through message encoding. The authors introduced an identity-based alphanumeric sign technique along with an improved homomorphism encryption scheme. The primary objective of this method was to detect and eliminate malicious codes during routing. The theory was validated on Mica Z motes, using RSA and oblique curve cryptography. To evaluate the results, metrics such as computational complexity, communication overhead, and energy consumption were used, though the paper lacks a comparison with other secure routing protocols.

A key management protocol for body area a network was proposed in [11], utilizing cryptanalytic confusion functions and a secure group key management framework. The results demonstrated improved confidentiality and mutual authentication between nodes in the proposed protocol. A similar study on group key security was discussed in [12], where the authors introduced a dynamic tunneling method to enhance group key management. The paper claimed low computational overhead and compared the proposed method with existing solutions like IPSec in terms of message volume and security delays.

In [13], a new public key cryptography-based security method was developed, incorporating covert originator information using oblique curve cryptography to enhance privacy in WSNs. Further, [14] introduced a key-based clustering policy using oblique curve cryptography along with alphanumeric signs. The study found that the system consumed minimal energy, making it energy-efficient. Additionally, research on WSN security and energy optimization was carried out in [15], focusing on related areas. A solution to resist wormhole attacks was proposed in [16], where the authors introduced a secure routing method that isolates compromised links upon detection.

The method involves analyzing the required conditions for identifying legitimate routes from tunnel encapsulation using the unit disk graph structure. The study's findings were compared with advanced methods to determine an effective packet delivery ratio. A study aimed at maximizing privacy in wireless sensor network data collection was presented by [17]. The primary objective was to reduce collision rates over random time intervals and develop a compensation mechanism for data loss.

A review of the literature also revealed that much of the existing research has focused on using graph theory to enhance security. A significant study [18] explored the implementation of symmetric encryption schemes tailored to the unique characteristics of sensor networks. The authors integrated a key management strategy with a spanning tree-based approach, and the study's outcome was evaluated based on the volume of messages exchanged relative to the size of neighboring nodes.

Further research investigated geographic-based routing protocols [19]. The proposed method utilizes a specialized localization process that helps detect intruders, followed by appropriate quarantine actions.

An interesting aspect of the study is that the secure routing algorithm it introduces is compatible with both ad hoc and sensor networks. The root mean square error was used to assess the accuracy of the system's positioning, and the results demonstrated reduced localization error through real-time testing with motes.
Another distinctive research study [20] focused on load balancing, applying security measures to protect communication channels within wireless sensor networks. The approach was further evaluated through simulation with 3000 sensors, focusing on defense against sinkhole and wormhole attacks.
The study also analyzed the number of received signals and the energy consumption of the sensors, which provided valuable insights into the network's performance. A reliable confidentiality-focused routing protocol was developed in [21]. While the study primarily emphasized web networks, the findings can also benefit sensor networks. Additionally, [22] provided a detailed analysis of sensor network security, with a particular focus on the importance and security implications of cognitive radio. Another innovative study [23] introduced a secure routing mechanism for underwater sensor networks, with the dual aim of enhancing security and conserving energy.
These studies demonstrate that ongoing research on wireless sensor network security is extensive, with each approach offering distinct advantages and limitations. The issues identified for the proposed study are discussed in the next section.

ISSUES WITH COMMONLY USED TECHNIQUES :
This section discusses the challenges identified through an evaluation of current vulnerability mitigation strategies for wireless sensor networks (WSNs). Research on security concerns in WSNs has been ongoing for over a decade.
There is always a trade-off between enhanced security and communication performance in sensor networks. As communication technologies advance, adversaries also develop more sophisticated methods, creating a constant struggle to maintain security. Before addressing the issues that have been identified, it is essential to understand the capabilities and types of the existing countermeasures.

COMMONLY USED COUNTERMEASURES:
In the past, mapping protocols have been developed for various studies to identify transmission areas within sensor networks that are blocked or congested [24]. These security measures are particularly effective in defending against denial-of-service (DoS) attacks in WSNs. To prevent Sybil attacks, some research [25] incorporates mathematical features into their defense mechanisms.
These methods utilize transistor source panels, location verification, and probabilistic pre-distribution of keys to detect and mitigate Sybil attacks. Additionally, some studies [26] focus on validating the routes formed as a result of flooding events in WSNs, employing both secret-sharing techniques and probability theory in the process.
Several studies have also endorsed the use of subjective key pre-distribution strategies. Optimization-based approaches—such as neural networks, genetic algorithms, ant-colony optimization, and particle swarm optimization—have been widely explored. The primary objective of these studies was to enhance encryption mechanisms. However, these optimization-based mitigation strategies tend to be expensive due to the high cost of maintaining strong encryption while minimizing key sizes. WSNs are often used for real-time data transmission and streaming across various applications [27]. Unfortunately, optimization-based algorithms demand significant computational resources, which can strain the system. As a result, these techniques are not well-suited for real-time applications.

Other approaches, including reputation-based schemes, game theory, trust-based frameworks, and temporal sequence methods, also rely on probability theory, sequence analysis, and decision-making models. While some of these methods may offer a high level of security under ideal conditions, they often struggle to perform effectively in real-world scenarios. Furthermore, many implementations seek security solutions that do not rely on cryptographic techniques. Although such solutions can achieve security goals, there are still no protocols that effectively balance robust security, efficient communication, and energy conservation within wireless sensor networks.

ISSUE IDENTIFICATION :

The following challenges have been identified within the proposed system:

Inefficient Use of Cryptography:

It is widely accepted that cryptographic techniques rely on multiple iterative stages of encryption and decryption. While these operations are essential for safeguarding against adversaries, they also contribute to significant energy consumption. The data or message processing involved in these cryptographic procedures leads to excessive power usage, particularly during the data fusion stage, which experiences unnecessary energy loss due to the increased demand on circuitry. As a result, there are limited cryptographic methods that address the issue of reducing energy consumption by minimizing processing requirements.

Imbalance between Energy Conservation and Security:

Achieving an optimal balance between energy conservation and security requires careful consideration of where security is applied—whether at the node level or through routing mechanisms. Most existing security research focuses heavily on node-level protection, with less emphasis on routing-based approaches. However, while routing-based security methods offer efficient authentication mechanisms, they often introduce considerable transmission delays. This makes it difficult to assess the effectiveness of security strategies without relying on the conventional radio-based energy model. In practice, many of the studies discussed in Section 2 do not employ this traditional radio-based model, leading to a noticeable gap between the effectiveness of existing security frameworks and the need for energy-efficient solutions.

Research Focused on Adversaries:

It is well understood that various types of adversaries, such as sinkhole, Byzantine, node capture, black hole, and wormhole attacks, pose threats to wireless sensor networks. Additionally, much of the current security research is highly specific to certain types of attacks, meaning that proposed solutions often target only one particular threat. Consequently, it is essential to develop a security system capable of detecting multiple attack types and formulating responses based on those patterns.

Many adversarial nodes tend to exploit nodes with lower remaining energy in order to compromise their authentication mechanisms. As a result, there is a notable lack of studies that utilize public key cryptography to create uniform authentication schemes.

Insufficient Benchmarking

The majority of existing research on security in wireless sensor networks fails to compare its energy efficiency with that of hierarchical energy-efficient routing protocols. Effective benchmarking could be achieved by contrasting the performance of proposed security measures with established energy-efficient routing systems. Implementing public key cryptography to secure energy-efficient routing methods in WSNs presents a significant computational challenge, as highlighted in the problem statement of the proposed study. The next section will address the proposed system designed to tackle these issues.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

PROPOSED SYSTEM :

In our prior paper, we discussed the existing secure and energy-efficient communication systems utilized in wireless sensor networks. Our latest approach, which we also introduced, enhances communication security in sensor networks through a tree-based methodology. Moreover, we have developed a strategy that prioritizes robust authentication. Previous investigations were primarily focused on security rather than energy efficiency. Hence, it was postulated that the application of cryptography could further enhance security. However, the use of cryptography may also affect energy conservation and increase computational complexity. Therefore, our objective was to propose a routing strategy that integrates a strong authentication method, termed Secure Anonymous Routing with Alphanumeric Sign (DSGARS).

The proposed system comprises three fundamental modules, as illustrated in the schematic diagram in Figure 1: (1) a novel lightweight encoding system utilizing public key cryptography, (2) an innovative numerical sign system designed to secure the routing communication validation process, and (3) a mechanism to ensure confidentiality in routing communication. DSGARS asserts that a sensor node employs elliptic curve cryptography to perform routing while signing the message.

By incorporating a unique alphanumeric sign system and a discrete anonymity scheme through elliptic curve cryptography, we enhance its versatility. The node-to-node verification mechanism utilized in the proposed DSGARS framework is based on the foundation established in our earlier studies.

The proposed system also introduces an innovative framework that incorporates a predetermined number of randomly selected sensors. These sensors actively modify the routing data. DSGARS ensures that no sensor, whether legitimate or malicious, discloses the private information of the communicating sensors during this process. By employing two distinct mathematical formulations solely for generating and authenticating signatures, DSGARS provides a dual layer of security. The primary objective was to ensure that DSGARS utilized static memory for both routing and executing security operations. The key contributions of the proposed study are as follows:

- Development of a routing protocol that effectively balances energy efficiency with security.
- Creation of a routing strategy that exclusively targets the destination node and allows communication to be encrypted using public key cryptography.
- Enhancement of elliptic curve cryptography to minimize internal complexity associated with private key generation and utilization.
- Implementation of a state-of-the-art alphanumeric sign system capable of generating and validating signatures during the routing process.

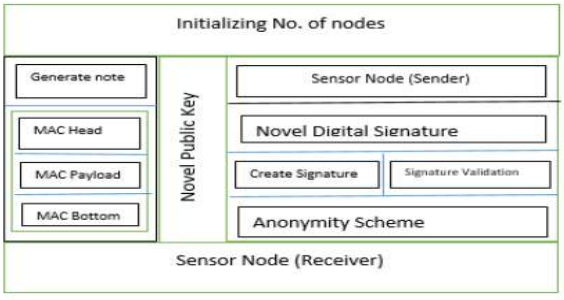


Fig 1: DSGARS for WSN

RESEARCH METHODOLOGY:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

The proposed DSGARS study employs an analytical research approach to address the domain of secure routing. While ensuring secure communication is the primary focus of DSGARS, the internal architecture of the suggested algorithm also ensures adequate energy efficiency. The fundamental framework for developing DSGARS is depicted in Fig. 2.

This figure illustrates a source and a destination, represented as two Cluster Heads (CHs) that are interconnected for the purpose of data aggregation. The transmitter generates a random number, combines it with ciphers and a hidden control message, and then sends the cipher to the next receiving node.

The receiving node will require a token or key to perform the decryption process. Given that there is a possibility that the recipient node could be a malicious one, authentication becomes essential. To fulfill this requirement, DSGARS requests an authentication token from the destination. Based on this token, the source determines whether to accept or reject the opportunity to route data with the receiver. The main components that make up the internal architecture will be elaborated on in this section.

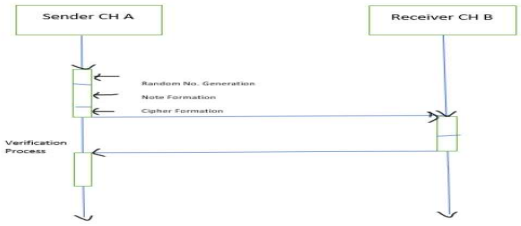


Fig 2: Fundamental DSGARS methodology

INNOVATIVE PUBLIC KEY CRYPTOSYSTEMS:

The proposed DSGARS approach utilizes public key cryptography and an elliptic curve foundation to encrypt messages, ensuring they reach only the intended destination. A sensor node typically initiates a message by broadcasting its values, which can be easily exploited by an adversary. The beacon is susceptible to spoofing, allowing an attacker to replicate it and compromise other sensors. To authenticate all collaborating nodes during the routing detection and validation phases, a robust public key is essential.

Our method leverages the positional data based on elliptic curves and is developed within finite fields. One of the significant advantages of elliptic curve cryptography over the commonly used RSA technique is its strong security coupled with a smaller key size. However, it also presents challenges due to its complex mathematical design, which can increase computational complexity and extend the range of the encrypted communication beyond what can typically be achieved with RSA and Diffie-Hellman encryption. Consequently, we implement specific adjustments to enhance the security features of elliptic curve cryptography. The encoding format of a message that can be utilized serves as the foundation for this innovative public key cryptography. We consider the message format of the beacon, as illustrated in Figure 3.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

Cluster	1	4 to 20	Var	2
Edge Regulator	Information Number System	Report Data	Information Load	Edge Sequential Checked
MAC H			MAC Load	MAC Bottom

Table 1: Beacon's data frame format in DSGARS

Cluster	1	2
Frame Control	Information Number Sequence	Frame Sequential Check
MAC Head		MAC Bottom

Table 2: Beacon's acknowledgement format in DSGARS

The previously mentioned message format comprises three primary fields: MAC header, MAC load, and MAC footer. However, the acknowledgment message does not include a payload. As a result, each message is assigned a unique and distinct identifier after it has been converted into a binary encoded format. It is possible that some elements within the binarized and encoded message may repeat. If these recurring elements are not addressed, the encoding method could become publicly accessible. To make it exceedingly difficult for an adversary to further decrypt the information, we enhance elliptic curve cryptography to identify such recurring patterns and appropriately substitute them with distinct encoded values.

Consequently, the enhancements made to traditional elliptic curve cryptography include the following: 1) Randomization of the third point of the elliptic curve, 2) Allowing the transmission of different beacons during each routing recognition and discovery attempt, and 3) Modifying the hashing process in conventional elliptic curve encoding by employing a binary communication structure to detect repeated cryptograms. Additionally, this system is fortified by an advanced alphanumeric signature mechanism.

INNOVATIVE ALPHANUMERIC SIGN FRAMEWORK:

The limited-area cryptanalysis reveals that elliptic curves form the basis of the public key cryptography approach employed by DSGARS. In cryptographic terms, elliptic curves essentially represent a specific cyclical subset, which leads to the equation (pk = q), where (p) and (q) are elements of a finite group. Consequently, we utilize the discrete logarithm of (k) to determine its value, a task that presents a significant challenge. The formation of private keys, or prime fields, results from applying various operations—such as preservation, multiplication, sharpening, and conversion—on elliptic curves. While this approach generates fewer keys, it can also lead to the creation of an excessive number of keys, potentially hindering computational efficiency. We have found that the discrete logarithm problem in cryptography lacks a standard solution.

The new alphanumeric signature framework comprises three main phases: 1) Secret key generation, 2) Secret signature development, and 3) Signature authentication. In this scheme, (alpha) and (beta) represent public and private key generators, respectively. The system computes the public secret key using the formula (k = beta r mod alpha).

Next, the system signs the secret message using a randomly selected secret key. The signature is generated using the equation (text{signature} = text{enc}(γcdot r cdot text{hash}(text{message}, γ) + l mod (alpha - 1))), where (l) is another random variable. The subsequent step involves verifying the secret signature using (beta text{signature} = γ^kcdot text{hash}(text{note}, γ) mod alpha). If the

signature is deemed valid, the system authenticates it and allows further communication. Any encryption algorithm can be utilized as the variable (text{enc}); however, we have opted for AES.

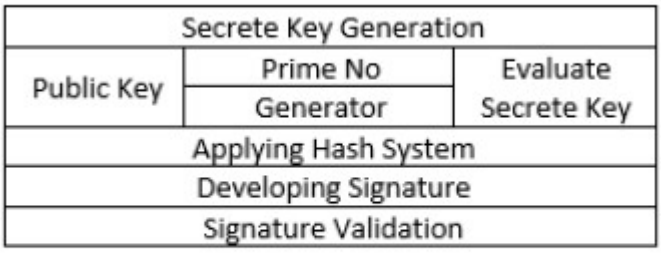


Fig 3: DSGARS alphanumeric sign system

NEWEST METHOD OF ANONYMIZATION:

The proposed DSGARS ensures that routing is conducted in a highly anonymous manner, such that only the sender and recipient nodes can access the original message. By maintaining complete anonymity, it prevents intermediary nodes from accessing private communications. The primary objective of this module is to guarantee total privacy. In this context, we also consider a memory component that stores sensitive data (such as cluster nodes, records, and loaded messages). To optimize memory usage, we assume this information is kept in a separate matrix, even though it resides within the nodes. The nodes involved in data aggregation will access this matrix. However, this functionality is restricted to communication between member nodes and the cluster head only. Consequently, we assume that any secret keys (of the public type) utilized in the encryption process must be registered within that matrix.

The ordering in Figure 6 illustrates the schematic diagram of the proposed anonymization system. The four entities in the scheme include the recipient, the alphanumeric signature, the elliptic curve matrix, and the transmitting nodes. The sender transmits the message along with a random number generator. A Fret encrypting all transactional data—including messages and secret keys—the matrix sends the encrypted information to be signed using the new alphanumeric signature technique. Once the message reaches the intermediate nodes, the originator's identity and the destination node address are encoded. We distribute the secret keys and encrypt the entire control message using the main module. As a result, the message is forwarded from one node to another without granting access to sensitive information to intermediate nodes.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

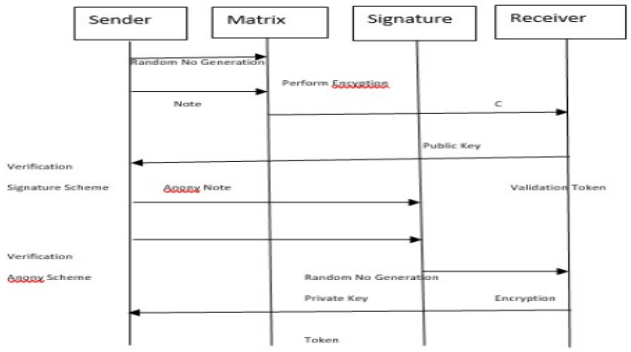


Fig 4: DSGARS anonymous program

ALGORITHM IMPLEMENTATION FOR DSGARS:

The proposed study utilizes MATLAB for its implementation. A simulation study is conducted within a wireless sensor network, considering a range of sensor counts from 50 to 500, utilizing both grid and random topologies. The simulation area for DSGARS is defined as 1200 x 1500 m². Additionally, the study does not rely on the location of the base station. Typically, the base station is situated in the center of the simulation area, following the hierarchical routing concept. However, we chose to abandon this concept, as placing the base station in the middle could lead to traffic congestion and complicate the scheduling of data packets directed toward the base station. Consequently, we positioned the base station as far from the cluster center as possible.

PUBLIC KEY CRYPTOGRAPHY ALGORITHM:

The input for this algorithm consists of a message of 2000 bytes, a transmission range (tx) of 10 m, and the number of nodes (n). The algorithm begins by computing two critical points, (a) and (b), on the elliptic curve. It also identifies the base point as the second point on the elliptic curve, (p).

Input:

- (n) (number of nodes)
- (br) (Broadcast Region)
- (S) (Simulation Domain)
- (note) (communication message)

Output: Encoding of the note

Start:

1. Initialize variables (m), (tr), and (S).
2. Evaluate parameters (a), (b), and the prime number (p).
3. Select a curve (c).
4. Sender A:
   a. Generate a random key (key_i).
   b. Calculate (key_i times c).
5. Receiver B:
   a. Generate a random key (key_j).
   b. Calculate (key_j times c).
6. Generate a random factor (SP).
7. Calculate (Key_i times Key_j times c times SP).
8. Set (Key_{priv} = y).

9. Convert the note to binary format.
10. If there is a duplication among broadcasted messages:
    a. Encode the note uniquely.
11. Encrypt the note using the formula: ((Key times note + p) mod p).
12. Decrypt the note using the formula: (((Step-8) times Key^{-1} + p) mod p).

End

ALPHANUMERIC SIGN ALGORITHM :

This algorithm addresses the use of asymmetric keys within encryption standards. In this context, (alpha) is an odd prime number that is always greater than three. The original equation of the elliptic curve is represented as (b^3 = a^3 + xa + y mod alpha), where (x), (y), and (alpha) are the variables involved. We also define (R) as a point on the curve, denoted as (R = (a_R, b_R)). As the sender's private key, the recipient must select a random number whose value lies between 1 and (N-1). Subsequently, the source calculates its public key.

Algorithm for Alphanumeric Sign:

Input:

- (note) (communication message)
- (N) (a standard number)
- (Ch) (a private share)

Output: Creation and verification of signatures

Start

1. Initialize arbint as a range from 1 to N-1.
2. Calculate γ as the modulo operation of rA by N.
3. Repeat the following steps until γ ≠ 0:

a. Generate a random number γ using arbint.

4. Hash the note using γ.
5. Calculate Ch as γ multiplied by dA hashed with hashA, plus keyA modulo N.
6. Repeat the following steps until Ch ≠ 0:

a. Generate a new random number γ using arbint.
b. Hash the note using the new γ value.
c. Calculate Ch again based on the new γ value.

7. Generate a alphanumeric sign dig_sig containing γ and sh.
8. Estimate hashA, r1, and r2 such that r2 = Ch F - γ hashed with hashA and multiplied by kpub.
9. If γ equals r1 modulo N, set dig_sig as valid; otherwise, set dig_sig as invalid.

End

ANONYMITY ALGORITHM:

Ensuring that the sent routing communication spreads its terminus while retaining a high level of secrecy is the major goal of the anonymity algorithm. The Alphanumeric Sign Algorithm

Input: *note* (message), N (natural number), Ch (covert share).

Output: creation and verification of signs.

Start:

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 1, No.1, January : 2025

1. Choose an arbitrary key key_i.
2. Compute γ_i and k_i as $(\gamma_i, k_i) = key_i \times F$.
3. Choose another arbitrary key key_t.
4. Compute γ_t and k_t as $(\gamma_t, k_t) = key_t \times F - \sum_i(\gamma_i, \text{hash}_i, \text{keypub}_i)$.
5. Calculate sh as $key_t + \sum_i key_i + (\gamma_t \times d_t \times \text{hash}_t) \mod Z$.
6. If (γ_i, k_i, I) is within the range $[0, Z-1]$, set Dig_sig as valid; otherwise, set Dig_sig as invalid.
7. Compute the hash value of msg and γ_i as $\text{hash}_i = \text{hash}(msg, \gamma_i)$.
8. Compute (r_o, k_o) as $shF - \sum_i(\gamma_i, \text{hash}_i, \text{keypub}_i)$.
9. If $\text{ic}(\sum_i(\gamma_i, k_i)) = r_o$, set Dig_sig as valid; otherwise, set Dig_sig as invalid.

Endγ

In the event of an internal or external attack on a sensor network, this technique provides two layers of security for the routing messages. The algorithm begins by selecting a random key (k_i) that falls within the range of 1 to (Z-1). Following this, the computation of (γ_i), an essential element of the alphanumeric signature, takes place. However, unlike the previous alphanumeric signing process, a different calculation method for (γ_i) is employed here to enhance the level of secrecy.

Although the same cryptographic hash function is utilized, the elements of the hash matrix are continuously changing, while the memory remains constant. This occurrence presents a significant advantage; even if we assume that an attacker gains access to the message, the information remains highly secure. An attacker would require multiple key standards to decode the communication, but these values are never accessible once the sender node transmits the message. Furthermore, a distinct technique is employed to calculate the secret share (sh), ensuring that no information can be extracted from the proposed DSGARS alphanumeric signature.

Essentially, the switch communication will consist of the message (msg) combined with a background containing the valid node report matrix, (γ_i), and (k_i). A similar approach will be used to verify the proposed signature. The process will solely authenticate (γ_i) and (k_i) from the entire message content to confirm that they fall within the range of 1 to (Z-1).

RESULTS AND DISCUSSION:

The results of the proposed study were compared against those of SLEACH, LEACH, and PSDCSIS, which are three traditional energy-efficient routing protocols commonly used in WSNs. The following outlines the findings of the study.

ENERGY EFFICIENCY ANALYSIS:

The findings of the study indicate that the proposed DSGARS exhibits considerably improved energy efficiency compared to existing schemes (Figure 7). Among the protocols analyzed, SLEACH is the only one that incorporates security measures, and it shows better energy conservation trends than LEACH upon a detailed examination of the energy curve. However, it is noted that the node consumes more energy than PSDCSIS due to the encryption process involved. DSGARS utilizes elliptic curve cryptography and alphanumeric signatures, but its approach is restricted to a 35-bit memory sharing, resulting in quicker processing times and reduced energy consumption.

To alleviate the typical demands of verification and communication duration, we maintain a dedicated medium that holds the valid and routing data. This method conserves approximately 0.35 watt-seconds during route verification and about 0.27 joules for each route discovery round. Thus, a substantial amount of energy is preserved during the signature generation and verification phases of the simulation study. Additionally, we found that DSGARS consumes relatively less energy even as traffic loads increase, especially when compared to current secure and energy-efficient routing techniques used in sensor networks.

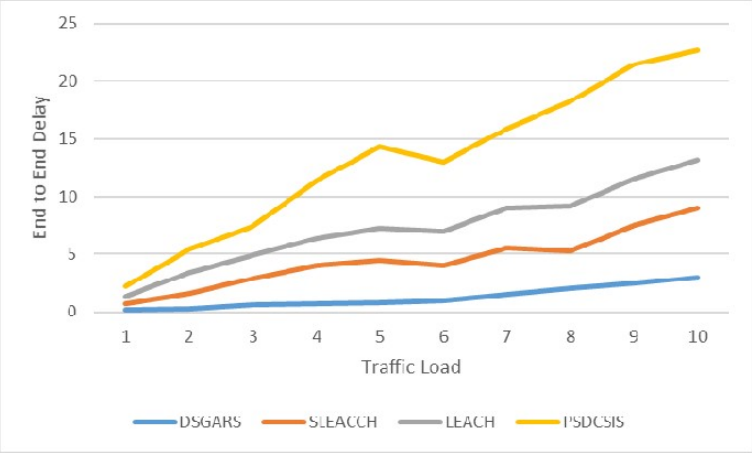
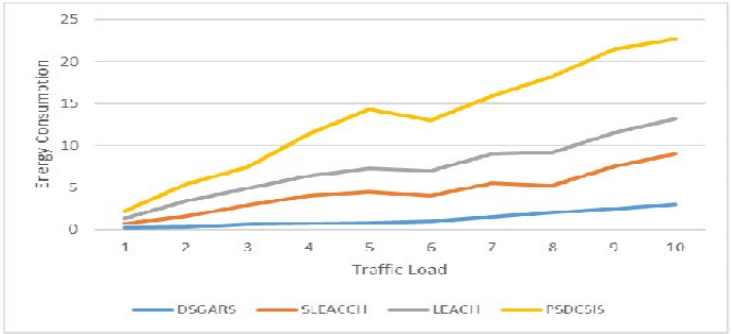


Fig 6: Energy Consumption analysis

END-TO-END DELAY ANALYSIS:

Another critical metric considered in the evaluation of the proposed DSGARS is end-to-end delay. Figure 8 demonstrates how the base station's location and the clustering process lead to a significant increase in delay for LEACH. While PDSCSIS provides a shorter delay compared to LEACH, it does not implement any security measures. SLEACH performs better than both LEACH and PDSCSIS; however, it incurs more overhead due to its reliance on a symmetric key management system. In contrast, DSGARS utilizes a combination of alphanumeric signatures and public key cryptography to address this issue. As a result, the overall authentication process is faster compared to existing methods, significantly decreasing the end-to



-end delay.

PACKET SENDING RATIO ANALYSIS :

Additionally, an assessment of the packet sending ratio was conducted on DSGARS to evaluate communication effectiveness. Table 1 presents the statistical results, indicating that DSGARS achieves a

higher packet distribution ratio compared to existing routing protocols such as SLEACH, LEACH, and PSDCSIS. To analyze whether nodes can manage the increased traffic load as the number of nodes grows, we incrementally raised the count from 100 to 1000.
Due to energy depletion, the trends in the packet delivery ratio showed a decline. Overall, the results demonstrate that DSGARS surpasses the current routing systems in terms of communication performance as well as security.

CONCLUSION :
This study addresses the weaknesses in authentication within wireless sensor networks (WSNs) by utilizing a public key encryption approach. It introduces a novel methodology called DSGARS, which features three innovative elements: 1) a new alphanumeric signature system, 2) a new public key encryption method, and 3) a new privacy or anonymity scheme. The findings reveal that DSGARS processes data at twice the speed of the existing routing methods discussed in this research. In addition to performance complexity, the system also measures storage difficulty based on the length of the message. Notably, the proposed system performs verification based on the total number of nodes in the simulated environment using a predetermined matrix. Consequently, the system requires less computational power and has simplified storage requirements. Furthermore, it has been shown that the performance of the proposed system is superior to that of the current protocols, including SLEACH, LEACH, and PSDCSIS.

REFERENCE :
1.Bramas Q, Tixeuil S. The complexity of data aggregation in static and dynamic Wireless Sensor Network.Springer Journals. 2015; 9212:36–50.
2. Wang L, Abu bucker CP, Washington W, Gilmore K. Mini- mum-latency broadcast and data aggregationscheduling in secured Wireless Sensor Network. Springer-Journal.2015; 9204:550–
3.Khan MA. Handbook of research on industrial informatics and manufacturing intelligence: Innovations andsolutions. IGI Global, Technology and Engineering; 2012. p. 662
4. Rahayu TM, Lee SG, Lee HJ. A secure routing protocol for Wireless Sensor Network considering secure dataaggregation.Sensors. 2015; 15(7):15127–58.
5. Das SK, Kant K, Zhang N. Handbook on securing cy- ber-physical critical infrastructure. Elsevier.Computers;2012. p. 848.
6. Toghian M, Morogan MC. Suggesting a method to improve encryption key management in Wireless SensorNetwork. Indian Journal of Science and Technology. 2015 Aug, 8(19):1–17. Doi no:10.17485/ijst/2015/v8i19/75986.
7. Biswas K, Muthukkumarasamy V, Singh K. An encryption scheme using chaotic map and geneticoperations for Wireless Sensor Network.IEEE Sensors Journal. 2015 May;15(5):2801–9.
8. Sasi SB, SivanandamN. A survey on cryptography using optimization algorithms in WSNs. IndianJournal of Science and Technology. 2015 Feb; 8(3):216–21. Doi no: 10.17485/ijst/2015/v8i3/59585.
9. Kasraoui M, Cabani A, Chafouk H. Collaborative key ex- change system based on Chinese remainder theorem in heterogeneous wireless sensor networks. Hindawi Publishing Corporation. 2015; 159518: p. 12.
10. Amalarethinam DIG, J. SaiGeetha J, Mani K. Analysis and enhancement of speed in public key cryptography using message encoding algorithm. Indian Journal of Science and Technology. 2015 Jul; 8(16):1–7. Doi no:10.17485/ ijst/2015/v8i16/69809.

11. Shen J, Tan H, Moh S, Chung I, Liu Q. Enhanced secure sensor association and key management in wireless body area networks. Journal of Communications and Networks. 2015 Oct; 17(5):453–62.
12. Bellazreg R, Boudriga N. DynTunKey: A dynamic distrib- uted group key tunneling management protocol forhet- erogenous Wireless Sensor Network. Springer-EURASIP Journal on Wireless Communications and Networking; 2014. P. 1–19.
13. Kodali RK. Implementation of ECC with hidden generator point in Wireless Sensor Network.IEEE; Bangalore.2014 Jan 6-10. p. 1–4.
14. Sahoo SK, Sahoo MN. An elliptic curve based hierarchical cluster key management in Wireless SensorNetwork. Springer.2014; 243:397–408.
15. Liu A, Yang LT, Sakai M, Dong M. Secure and energy-effi- cient data collection in Wireless Sensor Network.Hindawi Publishing Corporation. 2013. 565076. p. 3.
16. Matam R, Tripathy S. WRSR: Wormhole-Resistant Secure Routing for wireless mesh networks. Springer -EURASIP Journal onWireless Communications and Network in; 2013 Jul.
17. Yang G, Li S, Xu X, Dai H, Yang Z. Precision-enhanced and encryption-mixed privacy - Preserving data aggregation in Wireless Sensor Network. Hindawi Publishing Corporation; 2013. 427275. p. 12.
18. Messai ML, Aliouat M, Seba H. Tree-based protocol for key management in Wireless Sensor Network. Hindawi Publishing Corporation. 2010.
19. Otero MG, Zahariadis T, lvarez FA, Leligou HC. Secure geographic routing in ad hoc and Wireless SensorNetwork. Hindawi Publishing Corporation. EURASIP Journal on Wireless Communications and Networking.
2010.20. Sheng WX, Zhao ZY, Min WL. Load-balanced secure rout- ing protocol for Wireless Sensor Network HindawiPublish- ing Corporation; 2013. 596352. p. 13.
21. V. Gowthami and G. Murugaboopathi “Safety Cubic Dimension Acoustic and Routing in Acoustic SensorNetwork” Journal of Ambient Intelligent and Humanized Computing– Vol No. 12, Issue No. 7, Page No. 7225 - 7234,ISSN 1868-5137, http://doi.org/10.1007/s12652-020-02397-x
22. Lin H, Ma J, Hu J, Yang K. PA-SHWMP: A Privacy-Aware Secure Hybrid Wireless Mesh Protocol for IEEE 802.11swireless mesh networks. Springer - EURASIP Journal on Wireless Communications and Networking.2012 Dec.
23. Fragkiadakis A, Angelakis V, Tragos EZ. Securing cognitive Wireless Sensor Network: A survey.InternationalJournal of Distributed Sensor Networks.2014, 393248.p. 12.
24. Singh DAAG, Leavline EJ. EERCM: Energy Efficient and Reliable Communication Model for achieving QoSinun- derwater sensor networks. International Journal of Energy, Information and Communications. 2013 Oct;4(5):35–44.
25. Wood AD, Stankovic JA, Son SH. JAM: A Jammed-Area Mapping service for sensor networks. 24th IEEE Real-Time Systems Symposium; 2003 Dec 3-6. p. 286–97.
26. Ye F, Luo H, Lu S, Zhang L. Statistical en-route filtering of injected false data in sensor networks. IEEE Journal onSe- lected Areas in Communications. 2015 Apr; 23(4):839–50.