DSGARS: Alphanumeric Sign-Based Secured Anonymous Routing in Wireless Sensor Network

Dr. Gowthami V [1] , Dr. Krishna Prasad [2]
Post-Doctral Fellow, Institute of Computer Science and Information Science, Srinivas University [1]
Assistant Professor, School of Sciences and Computer Studies, CMR University[1]
Professor and Head, Department of Cyber Security and Cyber Forensics, Institute of Engineering and Technology, Srinivas University, Mukka, Mangaluru, Karnataka, India [2]

Abstract

In recent periods, there has been a significant amount of study on energy efficiency and security in wireless sensor networks. Few research, nevertheless, have found a secure routing method that is both economical and energy-efficient to yet. Our goal is to ensure energy effective routing in WSNs by using public key cryptography. The suggested work describes a method known as DSGARS (Alphanumeric Sign-Based Secured Anonymous Routing in Wireless Sensor Network), which proves the routing data that is shared between sensors in a wireless sensor network. DSGARS achieves verification of entire collaborating nodes in network and uses oblique curve cryptoanalysis as the foundation of safety preparations. By proposing a original sign based technique in the direction of public significant encoding strategy, the system also permits a second layer of security. The study's conclusion demonstrates that, when related to other safety and energy effective routing systems, DSGARS performs the best. The suggested DSGARS method provides Three new schemes: 1) a alphanumeric sign scheme, 2) a privacy or anonymous scheme, and 3) a public key encryption technique. Additionally, it is discovered that the suggested system's performance is better than that of the current protocols, such as SLEACH, LEACH, and PSDCSIS.

Keywords: SLEACH, LEACH, PSDCSIS

Introduction

In situations where human-oriented intervention is impractical, such as atomic shrub nursing, territory nursing, weather investigation, woodland fire recognition, etc., wireless sensor networks are mostly used. Typically, in these areas, sensors are dropped from airplanes at low altitude with the primary objective of performing environmental sensing, such as motion, temperature, heat, pressure, and smoke. Data aggregation is the method by which these sensors gather information and direct it to the improper place [1,2]. On the further pointer, a sensor's limited computational capacity, low processing power, small buffer, etc. But before the single information is sent to the following cluster head and ultimately the base station, it must first pass through a data fusion process that reduces redundancies using a voting system and specific statistical techniques. Such processed data is extremely important and useful information for some unauthorized parties, sometimes known as adversaries. An enemy node in a wireless sensor network may be installed after the sensors are deployed or it may already be present in the monitoring region. A more thorough examination of the theory and fiction exposes that frequent trainings have been conducted on the problems of energy efficiency and routing protocol in sensor networks [3]. But before the single information is sent to the subsequent CH and ultimately the improper place, it must first pass through a data fusion process that reduces redundancies using a voting system and specific statistical techniques. Such processed data is extremely important and useful information for some unauthorized parties, sometimes known as adversaries. An enemy node in a wireless sensor network may be installed after the sensors are deployed or it may already be present in the monitoring region. A more thorough examination of the theory and fiction exposes that frequent trainings have been conducted on the problems of energy efficiency and routing protocol in sensor networks [4].

Since sensor networks employ remote access policies as well, their privacy is extremely susceptible to compromise. Sophisticated cryptography could not be installed on a sensor node due to computing limitations. Effective cryptographic protocols must also guarantee efficient non-repudiation, confidentiality, privacy, integrity, and authentication. Because of this, the bulk of instructors who have been occupied on security systems to date have focused more on routing-based methods than node constructed systems. While cryptographic techniques based on node constructed systems are unable to maintain security for an extended period of time, those applicable to routing constructed systems require energetic retention in order to stock and apply the significant organization protocol [5]. Therefore, a reliable authentication technique must be ensured by a cost-effective security system. Additionally, it was discovered that public significant cryptoanalysis is the most cost-effective and lightweight encryption approach; nonetheless, even the keys produced by this process are not harmless because they must be broadcast to the target node. The provision of a safe encryption technique has already promoted seriously from the application of oblique curvature cryptography. However, in the field of WSNs, oblique curve cryptoanalysis's durability and economic viability remain in doubt. As a result, the current study develops a strong authentication mechanism between nodes. The study maintains a well stability among energy effectiveness and safety resilience by implementing a public key encryption scheme at a low cost. The paper offers a unique public key cryptography system and a novel sign technique with the goal of resolving current security difficulties. After discussing earlier security technique literature in Sector 2, Sector 3 addresses problem identification. Sector 4 provides an overview of the proposed system, while Sector 5 delves deeply into the study process. The discussion of algorithms takes place in Sector 6, and the discussion of results takes place in Sector 7. The paper is summarized in Sector 8.

2. Related Work

The research being done for secure communication in WSN is covered in this sector. The popular of [6] have accessible recommendations for how to enhance wireless sensor network encryption key management. Hashing is another method the authors utilized to reduce latency. It was also exposed that energy efficiency was achieved if MD5 encryption was used. The authors haven't, however, contrasted the results with any already-existing solutions. [7] has described an encryption method that combines evolutionary algorithms with chaotic maps. The authors have verified the authenticity of the active sensors using public key cryptography (such as the oblique curvature). Real sensors were used in the experiments to see whether the planned method outperformed the advanced block ciphering algorithm. It's interesting to note that the authors tested the technique's effectiveness using entropy, CPU cycles, and memory consumption using image data. An overview of cryptography in WSNs utilizing optimization techniques is found in [8,9] has provided their research on communication security in heterogeneous sensor networks. The study also highlighted the issue of energy usage and, in the end, provided a framework for key exchange.

It suggests research on the use of message encoding in cryptography to increase speed in public [10]. The authors have introduced an identity-based alphanumeric sign technique and an improved homomorphic encryption scheme. Finding and getting rid of the malicious codes in routing was the technique's main goal. With mica Z motes, the theory was evaluated using RSA and oblique curvature cryptography. Computational complexity, communication overhead, and energy usage were employed to calculate the study's result. However, benchmarking against alternative secure routing protocols is absent from the paper. Using a event learning of a body area network, [11] has given a significant organization method utilizing cryptanalytic confusion role and significant organization protocol resulting to protected cluster significant group. The result demonstrated the effective advancing confidentiality and shared verification between the nodes of the proposed protocol. A study akin to this one on group key security was also provided [12]. A dynamic tunneling procedure has been provided by the authors to improve group key management. Additionally, the paper asserts to have little computational difficulty. The training was contrasted with current methods, such as IPSec, in terms of message volume and security delay. It has created a novel public significant cryptoanalysis security method [13]. The method that was provided was also combined with a covert originator fact using oblique curvatures to improve the privacy protocol in wireless sensor networks. It has introduced an oblique curvature cryptography-based key-based clustering policy [14]. Alphanumeric signs are also used in the study. It is also found that the system uses very little energy. It has also conducted research in a similar part of wireless sensor network safety and energy effectiveness [15]. It conducted research on wormhole attack resistance [16]. The writers have introduced a secure routing method that separates the compromised links after recognizing them.

The method requires analysing the necessary state for recognizing tracks that are permitted from tunnel encapsulation using the unit disk graph structure. The study's findings were related with the advanced method to determine the effective packet delivery ratio. A study to maximize privacy in wireless sensor network data collection has been provided by [17]. The key area is to reduce the collision rate over arbitrary time intervals and to develop a method for compensating data. The literature research has also exposed that the greatest amount of work has been done to use graph theory for security. It conducted a noteworthy study whereby emphasis was placed on the implementation of symmetric encryption schemes that are compatible with the unique attributes of sensor networks [18]. The authors have combined a key management technique with a spanning tree-based approach. The amount of message in relation to neighbour size was used to evaluate the study's outcome. It conducted studies regarding the use of geographic-based routing protocols [19]. The method being presented practices a special localization process that helps the handler recognize the invaders, after which the scheme takes the required quarantined actions. The study's intriguing aspect is that the safe routing algorithm it presents can be used with both ad hoc and sensor networks. The root mean square error was used to assess the study's positioning outcome. The results of the investigation showed reduced location error since motes were used for real-time experimentation. It provided yet another distinctive collection of research [20]. The solution that was presented focused mostly on load balancing and employed security measures over the wireless sensor network's communication channel. Using 3000 sensors, the method was further evaluated for sinkhole and wormhole attacks during a simulation-based investigation.

The number of signals received and the sensors' energy ingesting were also examined in the learning's results. It work has produced a reliable confidentiality aspect routing protocol [21]. Despite the study's emphasis on web networks, sensor networks can also benefit from its application. It has provided an in-depth analysis of sensor network security, highlighting the importance of cognitive radio and its security implications [22]. It revealed yet another original study, this time offering a secure routing mechanism over underwater sensing [23]. The goal of the study is to achieve energy conservation as well. As a consequence, it is obvious that frequent research schemes pertaining to wireless sensor network security are underway. Each learning has its own benefits and potential drawbacks. The matters that have been recognized for the planned training are covered in the following sector.

3. Issues with Commonly Used Techniques

This sector addresses the matters that were initiate after an assessment of the present vulnerability mitigation strategies for wireless sensor networks. More than a decade has passed since the learning of safety concerns in WSNs began. There is always a skill off among improved safety and communication concert in the context of sensor networks because as communication systems evolve, the adversary also advances. Prior to talking about the matters that have been recognized, it is crucial that we comprehend the potential of the present countermeasures and their forms.

3.1 Often Utilized Countermeasures

Mapping protocols have been devised in the past for a variety of investigations to identify the transmission zones inside the sensor network [24] that are jammed. Security procedures of this type are well-suited to defend against attacks of service Denial in sensor networks. In order to fend off a Sybil assault, certain research [25], consume secondhand arithmetical features in their justification designs. To detect and thwart Sybil attacks, these methods employ transistor source panels, confirmation of location, chance significant pre delivery, etc. Additionally, we have located studies [26] that validate the tracks that are being built as a consequence of the overflowing occurrence in WSNs. Such methods are initiate to use both secret sharing and probability theory. There are frequent trainings that support the acceptance of a subjective significant pre delivery. Numerous research employing optimization techniques such as neuronal networks, inherent algorithms, ant-colony optimization, element group optimization, and others have been conducted. The primary goal of all these investigations was to optimize the encryption scheme; unfortunately, these optimization-based mitigation strategies come at a high cost. Nevertheless, it was a somewhat costly procedure to maintain maximum encryption and a smaller key size. Wireless sensor networks support real-time streaming and transmission processes in a variety of applications [27]. Regretfully, this method maximizes the use of resources to carry out the computation that optimization-based algorithms will need. Therefore, it is not advised to use these optimization-based techniques for real-time applications. There are other methods as well, such as reputation-based schemes, game theory, trust-based schemes, and period sequence approaches, which all need the application of probability theory, period sequence analysis, and policymaking values. Certain of them are probably going to have the highest amount of security possible based on conventions that don't grasp correct in a actual setting. Furthermore, these executions are constantly looking for security solutions that don't rely on cryptography. Although it accomplishes its security goal, we haven't yet encountered any protocols that effectively balance strong security, effective communication, and energy efficiency in wireless sensor networks.

3.2 Issue Recognition

The following issues with the suggested system are being noted:

3.1.1 Use of Cryptography Is Ineffective

It is a broadly apprehended acceptance that by means of different iterative levels of encryption and decryption is the result of a cryptographic technique. While these cryptographic operations are vital for protective compared to adversaries, the processing of data or messages they involve also results in excessive energy usage. Due to this circumstance, the data fusion stage itself experiences undesired energy dissipation due to increased circuitry power consumption. Thus, there aren't many cryptographic techniques that talk about how using less energy because of fewer processing

3.1.2 An Unbalanced Approach to Energy Conservation and Security

Understanding the point at which safety is applied—whether it be node constructed security—is crucial when working on safe and energy-efficient techniques. Node-based security is used in the majority of security research now in publication, with routing-based security receiving less attention. Routing-based security techniques, on the other hand, have a considerable transmission delay but efficiently allow authentication schemes. Therefore, it is actual problematic to determine the effectiveness of security without relying on the conventional radio-based energy model. In actuality, the traditional radio-based communication model is not used in the majority of the experiments covered in the preceding Sector 2. Consequently, there is a significant disparity between the current safety scheme and energy efficiency.

3.1.3 Research Particular to the Opponent

It is widely recognized that while studying wireless sensor networks, here, many dissimilar kinds of adversaries, such as sinkhole, Byzantium, node capture, blackhole, and wormhole attacks. Furthermore, a lot of the security research that is currently available is highly attacker-specific. This implies that the suggested remedy is limited to a only type of assault. As a effect, developing a security system that can identify diverse attack types and develop a response based on those patterns is crucial. Additionally, the bulk of the adversary nodes were seen to try and compromise the authentication mechanism of a node with less remaining energy in instruction to victimize it. As a outcome, fewer studies using public key cryptography to implement uniform authentication schemes have been observed.

3.1.4 Inadequate Use of Benchmarking

The mainstream of research on safety in wireless sensor networks that are now available does not compare its energy efficiency to that of hierarchical energy-efficient routing protocols. A useful benchmarking might be performed by contrasting the output that is provided with energy-efficient routing systems and security measures. This is a computationally interesting duty to practice public significant cryptoanalysis for safeguarding energy effective routing method in WSN, reads a problem statement of the proposed study. The system that was suggested in demand to report the aforementioned complications is covered in the following sector.

4. Proposed System

In our previous paper, we talked about the secure and energy-efficient communication systems that are already in use in wireless sensor networks. Our most recent method, which we also presented, secures communication in sensor networks by means of a tree-based methodology. Additionally, we have presented a method that emphasizes strong authentication. Our previous investigate has been a lesser amount of worried with energy efficiency and more with security. Therefore, it was believed that cryptography could improve security even more. Using cryptography, however, may also impact energy conservation and raise computing complexity. Therefore, our goal was to present a routing strategy that integrates a strong authentication method. It's called Secure Anonymous Routing with Alphanumeric Sign, or DSGARS for short. The planned system contains three core modules, as depicted in Figure1 schematic diagram: 1) a original trivial encoding system utilizing public significant cryptoanalysis; 2) a original numerical sign system for safeguarding the routing communication validation process; and 3) to confirm confidentiality in the routing communication. DSGARS claims that a sensor node uses oblique curvature cryptography to conduct routing while signing the message. By adding a unique alphanumeric sign system and a discrete anonymity scheme by means of oblique curvature cryptoanalysis, we increase its versatility. The same node to node verification device used in the proposed DSGARS scheme is based on our previous studies' framework.

An innovative background that holds a predetermined amount of arbitrarily selected sensors is also introduced by the suggested system. These sensors make dynamic changes to the routing data. DSGARS makes sure that no sensor, whether regular or malicious, ever divulges the private information of the communicating sensors while carrying out this activity. By employing two distinct mathematical formulations only to generate and authenticate signs, DSGARS offers a twofold layer of security. The main goal was to make sure that DSGARS used static memory for routing and executing security operations.

The subsequent are the core charities of the suggested study:

- Creating a routing protocol that can effectively balance energy efficiency and security.
- To create a routing strategy that only targets the destination node and enables the communication to be encoded by means of public significant cryptoanalysis.
- To improve oblique curvature cryptography in order to reduce internal complexity related to private key creation and usage.
- To put into practice a cutting-edge alphanumeric sign system that can be used to generate signs and validate them while the routing process is underway.

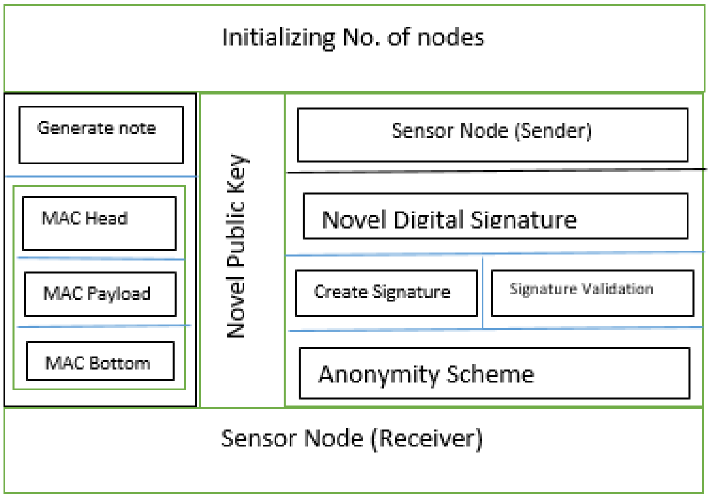


Fig 1: DSGARS for WSN

5. Research Methodology

Analytical research approach is used in the suggested DSGARS study to accomplish the area of secure routing. While achieving secure communication is the key area of the DSGARS, the suggested algorithm's internal architecture also guarantees sufficient energy efficiency. The fundamental approach used to create DSGARS is illustrated in Fig2. It displays a source and a destination, which are effectively 2 CH that are associated to one alternative in instruction to aggregate data. The transmitter creates a random number, combines ciphers with a covert control message, and sends the cipher to the subsequent getting node. Though, a token or key will be required by the receiving node in instruction to carry out the deciphering procedure. Given the circumstances, there is a possibility that the recipient node is a rogue node, hence authentication is necessary. In order to complete this duty, DSGARS requests a authentication nominal from the destination, depending on which the source decides whether to accept or deny the possibility of routing with the receiver. The main modules that comprise the internal architecture will be further explained in this sector.

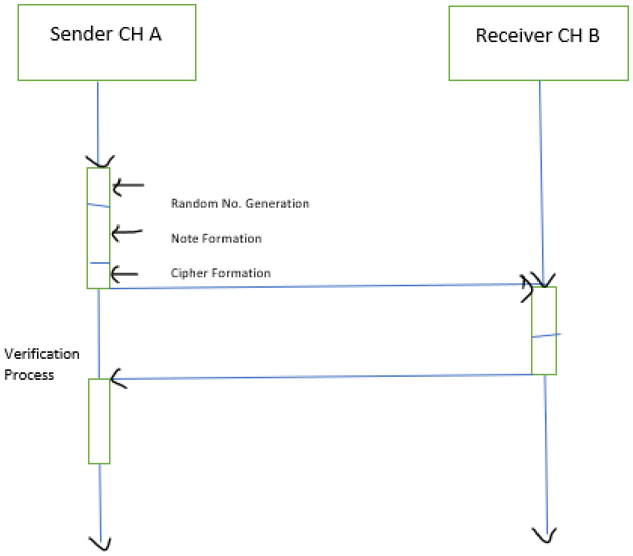


Fig 2: Fundamental DSGARS methodology

5.1 Innovative Public Key Cryptosystems

The suggested DSGARS approach encrypts messages so they only reach the destination address using public key cryptography and the base of an oblique curvature. A sensor node essentially initiates message by spreading its ideals, which an adversary may easily exploit. The beacon is easily spoofable, and an opponent can easily replicate it to attack other sensors. In order to validate the whole collaborating node during the route detection and validation phase, a strong public key can be helpful. Our method uses the positional data of the detail dwelling on oblique curvatures and is created on finite fields. Sturdy security and a reduced key size are two of oblique curvature cryptography's best qualities over the widely used RSA technique. It is accompanied, nevertheless, by problems with a convoluted mathematical design process that can escalate computational complexity and maximize the scope of the ciphered communication beyond what can be achieved by means of RSA and Diffie Hellman encryption. Therefore, we make certain adjustments to improve oblique curvature cryptography's security criteria. The encoding format of a message that may be viable is the foundation of the innovative public key cryptography. We take into account the beacon's message format (Figure 3).

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

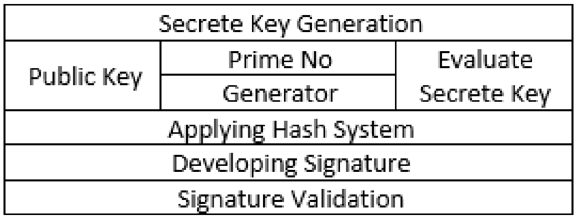
Cluster	1	2
Frame Control	Information Number Sequence	Frame Sequential Check
MAC Head		MAC Bottom

Table 2: Beacon's acknowledgement format in DSGARS

The message format mentioned above demonstrates the existence of three basic fields: MAC H (header), MAC load, and MAC footnote. Nevertheless, the acknowledgement message lacks the payload. Because of this, each message will have a unique and distinct number after it has been converted to a binarized encoded format. It is possible, though, that some of the mechanisms in the message that has been binarized and encoded may be repeated. If these repeating parts are not fixed, the encoding strategy may become public knowledge. In order to make it nearly hard for an adversary to decrypt it further, we improve oblique curvature cryptoanalysis to recognize such repeating cyphers and replace them appropriately with detached encoded codes. Therefore, the improvements made over traditional oblique curvature cryptography are as follows: 1) Randomization of the oblique curvature's third point, 2) Permits the transmission of distinct beacons during each attempt at route recognition and discovery; 3) Modifies the hashing process in traditional oblique curvature encoding using a binarized communication setup to detect recurring cryptograms. It is additionally protected by a cutting-edge alphanumeric sign system.

5.2 Innovative Alphanumeric Sign Framework

Limited arena cryptoanalysis concluded oblique curvatures serves as the foundation for the public key cryptography approach used by DSGARS. But in cryptography, oblique curvatures are essentially a kind of cyclical subcategory that result in the issue pk = q, where p and q are finite group elements. Therefore, we employ the discrete logarithm of k to find its value, which turns into a difficult problem to solve. Prime fields, or the formation of private keys, result from the request of numerous preservative, multiplicative, sharpening, and conversing operations on oblique curvatures. While the main benefit is that fewer keys are generated, this also results in a great quantity of keys being generated, which could slow down calculation. We discovered that the discrete logarithmic issue in cryptography lacks a benchmarked solution.



<table>
<tr><td colspan="3">Secrete Key Generation</td></tr>
<tr><td rowspan="2">Public Key</td><td>Prime No</td><td rowspan="2">Evaluate
Secrete Key</td></tr>
<tr><td>Generator</td></tr>
<tr><td colspan="3">Applying Hash System</td></tr>
<tr><td colspan="3">Developing Signature</td></tr>
<tr><td colspan="3">Signature Validation</td></tr>
</table>

Fig 3: DSGARS alphanumeric sign system

The new alphanumeric sign scheme consists of 3 basic phases: 1) Secret key generation scheme, 2) Secret significant development, and 3) Sign authentication. The scheme views alpha α and beta β as public generating prime number and private key generators, respectively. Next, the system uses k = βr.mod α to calculate the public secret key. The secret message message is then signed by the system using an arbitrary secret key that it selects. The development of the sign, represented as signature = enc (γ.r.hash (message, γ)+l.mod. (α-1)), somewhere l is an additional random quantity, will be the next step in the implementation. The study's following step involves validating the secret sign using β signature = γk\}.hash(note, γ).mod α. If the sign appears to be authentic, the scheme verifies it and permits additional communication. Any encryption algorithm might be used as the variable enc, however we chose AES.

5.3 Newest Method of Anonymization

The suggested DSGARS makes sure that routing occurs in a highly anonymous manner and that only the sender and recipient nodes can view the original message. By upholding total anonymity, it doesn't flat allow intermediary nodes to admittance the private communication. This module's primary goal is to ensure total privacy. In this regard, we also take into account memory that will store the protected significant data (cluster nodes, records, loaded significant, etc.). In order to save memory consumption, we presume that this information is stored in a separate matrix even if it is stored in nodes. The nodes that want to do data aggregation navigate to this matrix. Nevertheless, we restrict this function to member node and cluster head communication only. Therefore, we have decided to presume that any secret keys (public type) used in the encryption procedure must be registered in that matrix. The ordering figure6 displays the schematic diagram of the suggested innovative anonymity system.

The four actors in the scheme are the recipient, the alphanumeric sign, the oblique curvature matrix, and the transmitting nodes. The message is forwarded by the sender along with a random number generator. After encrypting all of the transactional data, including messages and secret keys, the matrix forwards the encrypted data to be signed using a brand-new alphanumeric sign technique. The originator's identity and the destination node address are encoded once the message has been received by intermediate nodes. We distribute the secret keys and encrypt the full control message using the main module. As a result, the message is then forwarded from one node to another without granting admittance truths to slightly nodes save the end point nodes. Thus, while routing utilizing DSGARS, an entirely reliable and lightweight encryption mechanism is suggested.

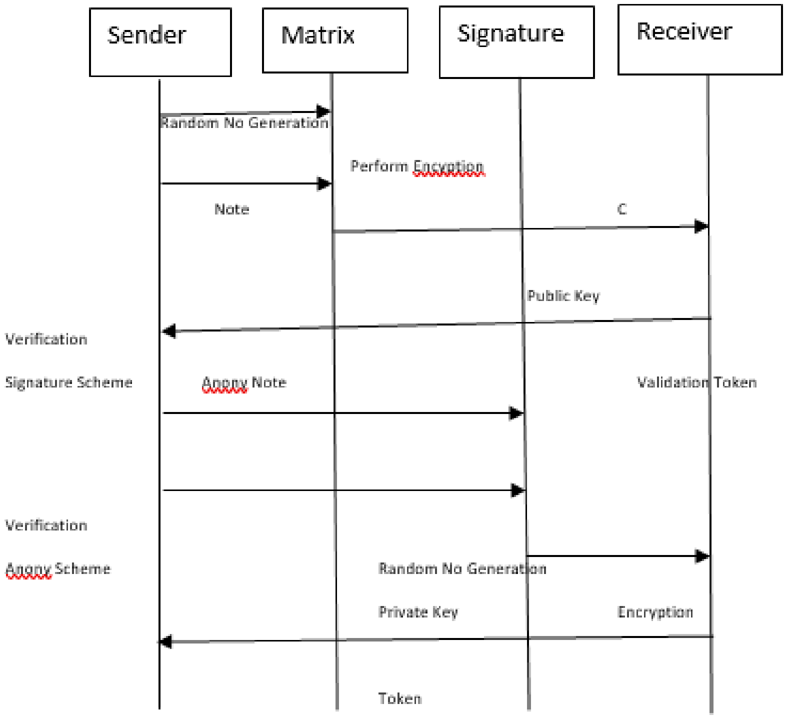


Fig 4: DSGARS anonymous program

6. Algorithm Implementation for DSGARS

Matlab is used in the preparation of the suggested study. In a wireless sensor network, the simulation study is conducted for a range of sensor counts, from 50 to 500, using both grid and random topologies. The 1200 x 1500 ^{m2} simulation area is taken into consideration for DSGARS. Additionally, the study is not dependent on the base station's location. Base station is typically located in the intermediate of the simulation region, inside the domain of the hierarchical idea of routing. We reject this idea because placing the base position in the middle could cause traffic jams and make it more challenging to schedule data packets to reach the base station. As a result, we positioned the improper position as far away from the group center as we could.

The algorithms used to create the suggested DSGARS are covered in this sector.

6.1 Public Key Cryptography Algorithm

The input for this algorithm is a message of 2000 bytes, a transmission area (tx) of 10 m, and the number of nodes (n). The two critical points, a and b, on the oblique curvature are first computed by the procedure. It also determines the base to be the second point on the oblique curvature, p.

Input: n (no. of nodes),

br (Broadcast Region)

S (Domain of Simulation)

note (communication).

Output: Encoding of note

```
Start
1. Initialize variables m, tr, S.
2. Evaluate parameters a, b, and the prime number p.
3. Choice a curve c.
4. Sender A:
    a. Generate a arbitrary key key_i.
    b. Estimate key_i * c.
5. Source B:
    a. Generate a random key key_j.
    b. Estimate key_j * c.
6. Generate an arbitrary fact SP.
7. Evaluate Key_i * Key_j * c * SP.
8. Cutting Key_priv = y.
9. Convert the note to binary format.
10. If here is a parallel design among broadcasted messages:
    a. Encode the note uniquely.
11. Encrypt the note using the formula (Key * note + p) mod p.
12. Decrypt the note using the formula ((Step-8) * Key^-1 + p) mod p
End
```

An random top-secret key key_i that falls among 1 and q is chosen by source node A. An analogous procedure is likewise executed on the alternative source node B. Lastly, the background Mat broadcasts to both nodes A and B instantaneously after choosing an chance fact SP. After calculating the secret key, the note is binary. We do discrete encoding if a parallel outline, sim_pat, is found in the note to make sure that no parallel kind of determined note is transmission. Lastly, the note is encrypted and decrypted.

6.2 Alphanumeric Sign Algorithm

The use of asymmetric keys in encryption standards is covered by this algorithm. According to the algorithm, α is an odd (primenumber) that is continuously superior than three. Assume that the original oblique curvature equation (b3 = a3+xa+y mod α) contains the variables x, y, and α. Additionally, we take R to be a position fact functioning in base, or R = (aR, bR). As the sender's private key, the recipient must select an chance figure whose worth falls between 1 and N-1. After then, the source calculates its community significant.

Algorithm for Alphanumeric Sign.

Input: note (communication), N (usual number), C_h (covertshare).

Output: creation and verification of signs

```
Start
1. Initialize arbint as a range from 1 to N-1.
2. Calculate $\gamma$ as the modulo operation of rA by N.
3. Repeat the following steps until $\gamma \neq 0$:
a. Generate a random number $\gamma$ using arbint.
4. Hash the note using $\gamma$.
5. Calculate $C_h$ as $\gamma$ multiplied by dA hashed with hashA, plus keyA modulo N.
6. Repeat the following steps until $C_h \neq 0$:
a. Generate a new random number $\gamma$ using arbint.
b. Hash the note using the new $\gamma$ value.
c. Calculate $C_h$ again based on the new $\gamma$ value.
7. Generate a alphanumeric sign dig_sig containing $\gamma$ and sh.
8. Estimate hashA, r1, and r2 such that r2 = $C_h$ F - $\gamma$ hashed with hashA and multiplied by kpub.
9. If $\gamma$ equals r1 modulo N, set dig_sig as valid; otherwise, set dig_sig as invalid.
End
```

The procedure stated above involves two crucial parts in its operation: the creation of a sign and its validation. A random integer, arbint, is chosen, and its value has to be among 1 and N-1. Lines 2 and 6 are used to estimate the two components of γ and C_h (covertshare), which are essential for each alphanumeric sign. Validation is necessary after the sign pair is created in Line-7. The algorithm first verifies whether keypub is a non-zero element, a single point inside the oblique curvature, or a path that goes to infinity before carrying out authentication. By verifying that γ and C_h are integer types and fall among 1 and N-1, the authentication is carried out. The hash function of node A must be determined in the second step, and r1 and r2 must be determined in the third phase using Line 8. As a result, the suggested DSGARS performs alphanumeric sign authentication with little reliance on network resources, and its size and memory usage are limited to 5–9 bits.

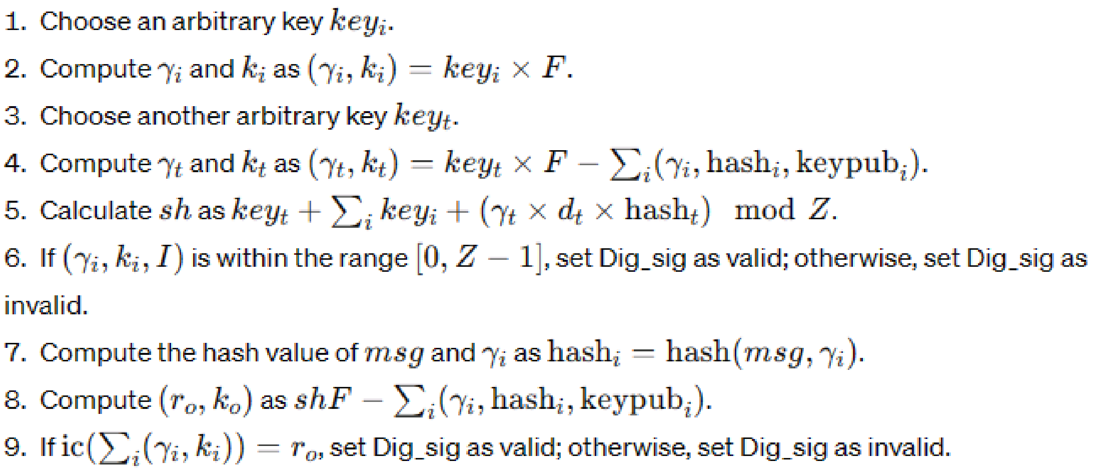
6.3 Anonymity Algorithm

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), C_h (covertshare).

Output: creation and verification of signs.

Start



```
1. Choose an arbitrary key $key_i$.
2. Compute $\gamma_i$ and $k_i$ as $(\gamma_i, k_i) = key_i \times F$.
3. Choose another arbitrary key $key_t$.
4. Compute $\gamma_t$ and $k_t$ as $(\gamma_t, k_t) = key_t \times F - \sum_i(\gamma_i, \mathrm{hash}_i, \mathrm{keypub}_i)$.
5. Calculate $sh$ as $key_t + \sum_i key_i + (\gamma_t \times d_t \times \mathrm{hash}_t) \mod Z$.
6. If $(\gamma_i, k_i, I)$ 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 $\gamma_i$ as $\mathrm{hash}_i = \mathrm{hash}(msg, \gamma_i)$.
8. Compute $(r_o, k_o)$ as $shF - \sum_i(\gamma_i, \mathrm{hash}_i, \mathrm{keypub}_i)$.
9. If $\mathrm{ic}(\sum_i(\gamma_i, k_i)) = r_o$, set Dig_sig as valid; otherwise, set Dig_sig as invalid.
```

End

In the event of an internal or external attack on a sensor network, this technique offers the routing message two levels of security. Initially, an arbitrary keyi is chosen by the algorithm so that its worth falls among 1 and Z-1. The calculation of (γi), a crucial component of a alphanumeric sign, comes next. But unlike the prior alphanumeric sign process, we use a different amount of calculation for γi here to ensure a higher level of secrecy. Because the same cryptographic hash function is used, the hash matrix's elements are constantly changing but the memory stays the same. There is one major advantage to this occurrence. Even if we suppose that an attacker has accessed the message, it is still quite secure. An attacker would need several standards of keys to decode the communication, yet these values are never available once the sender node has broadcast the message. Additionally, we use a separate technique to calculate secret share sh, ensuring that no information can be extracted from the suggested DSGARS alphanumeric sign. Basically, switch communication will be communication msg + a background with valid node report mat, γi, and keyi. A alike methodology will be applied to validate the suggested sign. The procedure will only authenticate γi and keyi from the complete message content to see if it falls among 1 and Z-1. Therefore, in Wireless Sensor Network routing message propagation, DSGARS substantially ensures the privacy component.

7. Results and Discussion

The suggested study's results were compared to those of SLEACH37, LEACH38, and PSDCSIS39, three traditional classified energy effective routing protocols used in WSN. The following are the study's findings.

7.1 Energy Efficiency Analysis

The study's conclusion demonstrates that the suggested DSGARS performs significantly better in terms of energy usage than the current scheme (Figure 7). Compared to LEACH and PSDCSIS, SLEACH is the one procedure that provides security. Upon closer inspection of the energy curve, SLEACH outperforms LEACH in terms of energy conservation trends. On the further pointer, the node uses more energy than PSDCSIS because of the encryption procedure. DSGARS employs oblique curvature cryptography and alphanumeric signs, but its process is limited to a 35-bit memory sharing, which leads to a faster processing time and less energy usage. In order to relieve the typical strain of verification and communication conversation period, we preserve a distinct medium that contains the valid data and routing data. The energy conservation of this procedure is about 0.35 Watt second during route verification and 0.27 Joules for each route finding round. Therefore, during the simulation study's sign production and verification phases, a considerable amount of energy is maintained. Additionally, we discovered that DSGARS use relatively less energy as traffic loads increase, even when related to current safety and energy effective routing approaches in sensor networks.

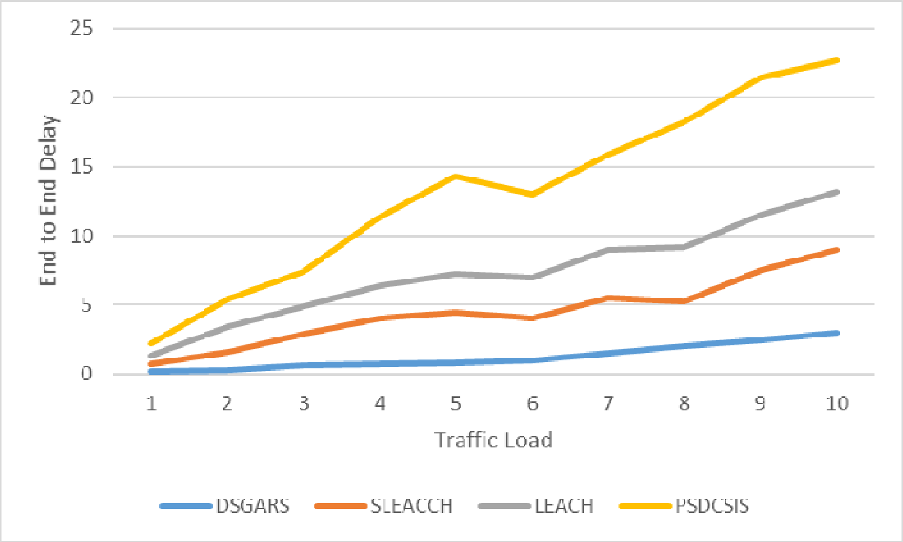


Fig 6: Energy Consumption analysis

7.2 End-to-End Delay Analysis

An additional concert system of measurement occupied into version when evaluating the suggested DSGARS is end-to-end latency. Figure 8 illustrates how the location of the base station and clustering process contribute to LEACH's noticeably growing delay. Compared to LEACH, PDSCSIS offers a shorter delay, but it lacks security policy. SLEACH outperforms LEACH and PSDCSIS, but because it uses a symmetric key management system directly, it has more overhead. The DSGARS uses a combination of alphanumeric sign and public key cryptography to solve this problem. In comparison to current techniques, the entire authentication process happens faster, greatly reducing the end-to-end delay.

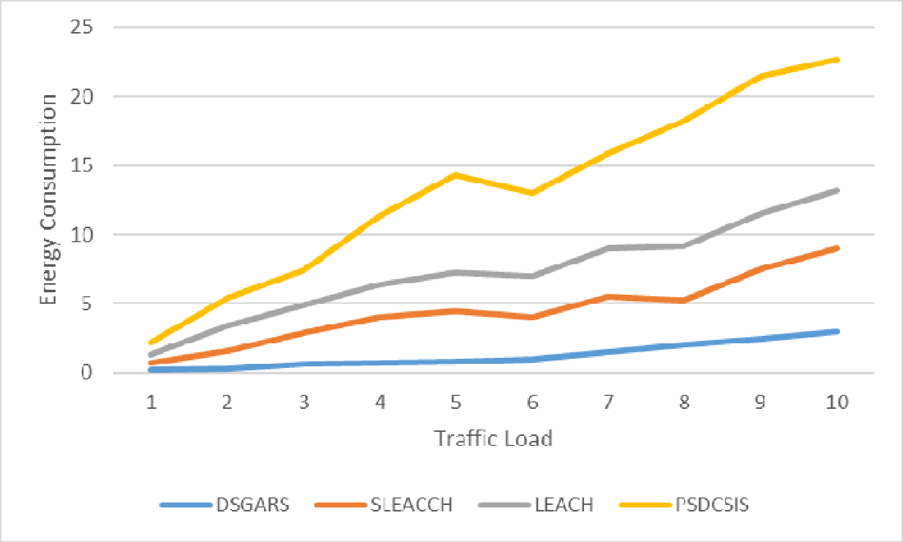


Fig 7: End-to-end delay analysis

7.3 Packet Sending Ratio Analysis

In addition, a packet distribution ratio assessment is approved out on DSGARS in instruction to verify the effectiveness of communication. Table 1 presents the arithmetical consequences, which designate that DSGARS has a advanced packet distribution ratio than the current routing protocols, such as SLEACH, LEACH, and PSDCSIS. In order to determine if nodes can adequately handle the traffic burden exerted by more nodes, we have progressively raised the number of nodes from 100 to 1000. Because of the energy drain, the trends in the packet delivery ratio are declining.
Consequently, the whole results demonstrate that DSGARS outperforms the current routing system in relations of communication performance as fine as security.

7.Conclusion

The public key encryption approach that is primarily intended to report the weak authentication problem in WSN is covered in this study. The method also presents a new methodology known as DSGARS, which provides three new features: 1) a original alphanumeric sign scheme, 2) a original public key encoding, and 3) a original privacy or anonymous scheme. It is discovered that the DSGARS processes data twice as quickly as the current routing methods covered in this research. By measuring the message's length, the system calculates storage difficulty in addition to performance-based complexity. The intriguing aspect of the suggested system is that it does verification founded on the whole amount of nodes in the simulated part using a predetermined matrix. As a consequence, the suggested system requires less computing power and has simpler storage. Additionally, it is discovered that the suggested system's performance is healthier than that of the current protocols, such as 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, Abubucker CP, Washington W, Gilmore K. Mini- mum-latency broadcast and data aggregation scheduling insecured Wireless Sensor Network. Springer-Journal. 2015;9204:550–60.
3. Khan MA. Handbook of research on industrial informaticsand manufacturing intelligence: Innovations and solutions.IGI Global, Technology and Engineering; 2012. p. 662
4. Rahayu TM, Lee SG, Lee HJ. A secure routing protocol forWireless Sensor Network considering secure data aggrega-tion. 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 improveencryption key management in Wireless Sensor Network. 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 encryp- tion scheme using chaotic map and genetic operations for Wireless Sensor Network. IEEE Sensors Journal. 2015 May; 15(5):2801–9.
8. Sasi SB, Sivanandam N. A survey on cryptography us- ing optimization algorithms in WSNs. Indian Journal 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 wireles sensor networks. Hindawi Publish- ing Corporation. 2015; 159518: p. 12.
10. Amalarethinam DIG, J. Sai Geetha J, Mani K. Analysis andenhancement 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 for het- erogeneous Wireless Sensor Network. Springer-EURASIP Journal onWireless Communications and Networking; 2014. P. 1–19.
13. Kodali RK. Implementation of ECC with hidden generatorpoint in Wireless Sensor Network. IEEE; Bangalore. 2014Jan 6-10. p. 1–4.
14. Sahoo SK, Sahoo MN. An elliptic curve based hierarchi- cal cluster key management in Wireless Sensor Network. 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. HindawiPublishing Corporation. 2013. 565076. p. 3.
16. Matam R, Tripathy S. WRSR: Wormhole-Resistant Secure Routing for wireless mesh networks. Springer - EURASIPJournal onWireless Communications and Networkin; 2013Jul.
17. Yang G, Li S, Xu X, Dai H, Yang Z. Precision-enhanced and encryption-mixed privacy - Preserving data aggregation inWireless Sensor Network. Hindawi Publishing Corpora- tion; 2013. 427275. p. 12.
18. Messai ML, Aliouat M, Seba H. Tree-based protocol for key management in Wireless Sensor Network. Hindawi Pub- lishing Corporation. 2010.
19. Otero MG, Zahariadis T, lvarez FA, Leligou HC. Secure geographic routing in ad hoc and Wireless Sensor Network. 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 Hindawi Publish-ing Corporation; 2013. 596352. p. 13.
21. V. Gowthami and G. Murugaboopathi "Safety Cubic Dimension Acoustic and Routing in Acoustic Sensor Network" 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-AwareSecure Hybrid Wireless Mesh Protocol for IEEE 802.11s wireless 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. International Journal of Distributed Sensor Networks. 2014, 393248. p. 12.
24. Singh DAAG, Leavline EJ. EERCM: Energy Efficient andReliable Communication Model for achieving QoS in un- 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 on Se-lected Areas in Communications. 2015 Apr; 23(4):839–50.
27. Hamid MA, Rashid MO, Hong CS. Routing security in sensor network: Hello flood attack and defense. IEEE IC- NEWS; Dhaka. 2006 Jan 2-4. p. 77–81.