ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(7), DOI: 10.17485/ijst/2016/v9i7/85760, February 2016* ISSN (Online) : 0974-5645

SARDS: Secured Anonymous Routing with Digital Signature in Wireless Sensor Network

H. R. Roopashree[1*] and Anita Kanavalli[2]

[1]Department of Computer Science and Engineering, Christ University, Bengaluru - 560029, Karnataka, India; roopashree.r@christuniversity.in
[2]Department of Computer Science and Engineering, MSRIT, Bengaluru - 560054, Karnataka, India; anithak@msrit.edu

Abstract

A Wireless Sensor Network has witnessed a massive research towards security as well as energy efficiency in past decades. However, there are few studies that have witnessed a cost effective secure routing technique with energy effectiveness till date. **Objectives:** Our objective is to use public key cryptography for ensuring energy-efficient routing technique in Wireless Sensor Network. **Method/Analysis:** The proposed paper presents a technique called as SARDS (Secured Anonymous Routing with Digital Signature) that performs verification of the routing information exchanged among the sensors in Wireless Sensor Network. SARDS uses elliptical curve cryptography as the backbone of security formulations and performs authentication of all the communicating nodes present in the network. **Findings:** The system also allows a dual layer of security by introducing a novel signature based scheme towards public key encryption policy. The outcome of the study shows SARDS to excel best in performance in comparison of existing security and energy efficient routing schemes. **Application/Improvements:** Proposed SARDS technique offers 1) A novel public key encryption, 2) A novel digital signature scheme, and 3) A novel privacy or anonymous scheme. The outcome of the proposed system is also found to be superior as compared to existing protocols e.g. SecLEACH, LEACH and PEGASIS.

Keywords: Attack, Public Key Cryptography, Security, Signature, Wireless Sensor Network

1. Introduction

Wireless Sensor Network is essentially used in those areas where it is not feasible for human-oriented intervention e.g. nuclear plant monitoring, habitat monitoring, climate surveillance, forest fire detection etc. Usually, in such area the sensors are dropped from aircraft in low elevation whose prime purpose is to perform sensing of environmental-based information e.g. smoke, temperature, heat, pressure, motion etc. These sensors collect information and forward it to the base station and this process is termed as data aggregation[1,2]. However, a sensor is characterized by minimal computational capability, low processing power, reduced buffer, etc[3]. However, the information extracted by the sensors are subjected to a process of data fusion, which uses voting system and certain statistical technique to reduce the redundancies and forward the unique data to the next cluster head and then finally to base station. Such processed information is highly valuable and serve as data of interest for some illegitimate member called as adversary. An adversary node may be present in advance in the area of monitoring or may be placed after the sensors are deployed in Wireless Sensor Network. A closer look into the theory and literatures have shown that there was a series of research towards energy efficiency problem as well as issues related to routing protocol in sensor network[4]. Although there are various forms of attacks in sensor network, majority of the attacks are related to authentication failures, energy depletion, routing problems etc, but few of them are found to provide an effective solution. The attacks related to jamming, denial of service, and corruption of message occurs at the physical layer[5]. The malicious replication and spoofing of routing data and sinkhole attack normally occurs in network layer. The origination of the Sybil attack only occurs when the identity of the network is compromised. The

* *Author for correspondence*

attacks related to flooding and synchronization normally occurs in transport layer[5]. As sensor network also uses remote access policies hence it is highly vulnerable towards privacy that can get compromised very easily. Owing to computational less compatibility, a sensor node couldn't be equipped with sophisticated cryptographic technique. An efficient cryptographic protocol must also ensure an efficient confidentiality, privacy, integrity, non-repudiation and authentication. Hence, majority of the existing researchers have presented security system more on routing based scheme and less on node based schemes. The cryptographic schemes applicable on routing based schemes requires dynamic memory to store and use the key management protocol, while cryptographic schemes based on node-based schemes cannot hold security for a longer time. Hence, there is a need of a cost effective security system that can ensure a robust authentication scheme. It was also seen that public key cryptography is the best option when it comes to cost and light weighted encryption scheme; however, even the key generated from the technique is not secured as such key are required to be broadcasted to the destination node. Usage of elliptical curve cryptography has already played a significant role in providing secure encryption scheme. But till date the robustness and cost effectiveness of elliptical curve cryptography is still questionable in the area of Wireless Sensor Network. Therefore, the present study formulates a robust authentication system from one to other nodes. The study implements a cost effective public key encryption policy in order to maintain a better balance between energy efficiency and security robustness. The study presents novel public key cryptographic scheme along with novel signature scheme that aims to resolve the existing issues of security. Section 2 discusses about the prior literatures towards security techniques followed by discussion of problem identification in Section 3. Section 4 introduces about the proposed system followed by an elaborated discussion of research methodology in Section 5. Algorithm discussion is carried out in Section 6 while result discussion is carried out in Section 7. Section 8 makes summarization of the paper.

2. Related Work

This section discusses about the existing research work being carried out for secured communication in Wireless Sensor Network.

Most reference[6] has suggested a method to improve encryption key management in Wireless Sensor Network. The authors have also used hashing technique for minimizing the latency. The outcome was also found to be energy efficient if encryption was carried out using MD5. However, the authors have not compared its outcome with any existing solution. Reference[7] have presented a technique of encryption using chaotic map as well as genetic algorithm. The authors have used public key cryptography (e.g. elliptical curve) in order to authenticate the active sensors. The experimentation was carried out on real sensors to find the presented technique to be better than existing block ciphering algorithm. Interestingly, the authors have used image data and tested the efficiency of the technique using CPU cycles, amount of memory consumption and entropy.

Reference[8] survey on cryptography using optimization algorithms in WSNs. Reference[9] has presented their study towards safeguarding communication over heterogeneous sensor network. The study have also emphasized over energy consumption issue and finally presented a key-exchange mechanism. Study towards enhancement of speed in public by cryptography using message encoding is proposed by reference[10]. The authors have presented an enhanced homomorphic encryption scheme along with identity-based digital signature technique. The prime purpose of the technique was to find and eliminate the malicious codes in routing. The assessment of the theory was done with mica Z motes using both RSA and elliptical curve cryptography. The outcome of the study was computed used energy consumption, communication overhead and computational complexity. However, the study misses benchmarking with other secured routing protocols. Reference[11] have presented a key management scheme using cryptographic hash function and key management protocol leading to secured group key generation using case study of body area network. The outcome proved the presented protocol to possess an efficient forward secrecy and efficient mutual authentication among the nodes.

Similar study towards securing group key was also presented by reference[12]**.** The authors have presented a dynamic tunneling process for enhancing the group key management. The study also claims to possess minimal computational complexity. The study was compared with existing technique e.g. IPSec with respect to message quantity and security latency. Reference[13] have developed a unique security technique using public key cryptography.

Using elliptical curves, the presented technique was also integrated with latent generator point for better privacy protocol in Wireless Sensor Network. Reference[14] have presented a key-based clustering policy using elliptical curve cryptography. The study also uses digital signatures. The system is found to also possess minimal energy consumption. Reference[15] has also carried out the study in similar direction of secure and energy efficiency in Wireless Sensor Network. Study towards resisting wormhole attack was carried out by reference[16]. The authors have presented a secured routing technique that is responsible for identifying the compromised links and then it segregates it. The technique calls for using unit disk graph framework for evaluating the required condition for identifying routes that are free from encapsulation of tunnel. The outcome of the study was compared with existing technique to find efficient packet delivery ratio. Reference[17] have presented a study to leverage the privacy factor in the process of data aggregation in Wireless Sensor Network. The prime objective is to minimize the rate of collision over arbitrary slots of time as well as technique to compensate data.

The review of literature have also witnessed maximum amount of work towards security using graph theory. One of such significant work was carried out by reference[18] where the focus was laid on using symmetric encryption scheme that goes well with the particular characteristics of sensor network. The authors have used spanning tree-based approach along with key management scheme. The outcome of the study was evaluated with respect to amount of message with respect to neighbor size. Studies towards usage of geographic-based routing protocol were carried out by reference[19]. Presented technique uses a unique localization procedure that assists the user for identifying the attackers and then the system performs necessary quarantined actions. The interesting part of the study is that the presented secure routing protocol can be applicable for both sensor network as well as ad-hoc network. The positional outcome of the study was evaluated with respect to root mean square error. With real-time experimentation being carried out over motes, the outcome of the study was found with less location error. Another unique set of study was presented by reference[20]. The presented technique mainly emphasized on the load-balancing technique and used security over the communication channel in Wireless Sensor Network. The technique was also tested for sinkhole and wormhole attack with 3000 sensors over simulation-based study. The outcome of the study was also checked for energy consumption of the sensors as well as amount of the messages being arrived. Work carried out by reference[21] has presented a robust privacy factor routing protocol. Although the study was focused on mesh network but it is equally applicable over the sensor network too. Reference[22] have presented a discussion towards security in sensor network that elaborates the significance of cognitive radio in sensor network and its security aspects. Another unique study was found to be presented by reference[23] by introducing a secure routing technique over underwater sensory. The study also intends to accomplish energy conservation. Therefore, it can be seen that there are various studies being carried out towards security in Wireless Sensor Network. All the studies have their own advantages and possible limitations too. The next section discusses about the problems being identified for the proposed study.

3. Problems with Frequently used Techniques

This section discusses about the problems being identified after reviewing the existing techniques of vulnerability mitigations Wireless Sensor Network. The study of security issues in Wireless Sensor Network is not new and is dated more than 10 decades ago. With the advancement of communication system, the adversary too upgrades themselves and hence a tradeoff between better security and communication performance in area of sensor network always exists. Before, discussing the problems being identified it is essential for us to understand what are the possible form of existing countermeasures and what are their potentials.

3.1 Frequently used Countermeasures

There are various studies in past where mapping protocol were developed in order to identify the transmission zone that are being jammed within the sensor network[24]. Such forms of countermeasures are well built for Denial-of-Service attacks in sensor network. Certain studies e.g. refrence[25] have also used statistical characteristics in the mitigation formulations in order to resist Sybil attack. Such techniques make use of radio resource controls, validation of localization, arbitrary key pre-distribution,

etc. in order to identify and resist Sybil attack. We have also found studies[26] that perform validation of the routes being established owing to the flooding attack in Wireless Sensor Network. Such techniques are found to adopt probability theory as well as secret sharing. Studies towards adoption of arbitrary key pre-distribution are also there. There are various studies carried out using optimization techniques neural network[27], genetic algorithm[28], Ant Colony Optimization[29], particle swarm optimization[30] etc. All these studies were mainly meant for optimizing the encryption scheme however such optimization based mitigation techniques are quite expensive. However, it was quite expensive process in order to retain lesser size of the key and maximal encryption. There are various applications in Wireless Sensor Network that supports real-time streaming and transmission process. Unfortunately, such process leads to maximized usage of resources in order to perform computation that will be required by the optimization-based algorithms. Hence, such optimization-based algorithms are not recommended for real-time applications. There also exists various other techniques e.g. trust-based schemes[31], reputation-based schemes[32], game theory[33], which calls for usage of stochastic-based theory, time-series, probability theory and decision-making principles. Some of them are likely to hold maximum level of security with certain assumptions that doesn't hold true in real-time environment. Moreover, such implementations are always in search of using non-cryptographic based solution to provide security. Although, it achieves its objective of security, but till date we didn't came across any such protocols that make a well balance between robust security, communication performance and energy efficiency in Wireless Sensor Network. Therefore, there is a serious need of a secure routing technique using lightweight encryption mechanism in order to overcome such diversified flaws and constraints.

3.2 Problem Identification

The problems being identified in the proposed system are as follows:

3.1.1 Ineffective about Cryptographic Usage

It is commonly believed that a cryptographic technique leads to use of various iterative levels of encryption and decryption. Although, such operations of cryptography is highly essential for security against an adversary but it also leads to excessive energy consumption owing to processing of data or message. This fact leads to more circuitry power usage leading to unwanted energy dissipation in data fusion stage itself. Hence, there is very less cryptographic technique which discusses about less energy consumption due to reduced processing.

3.1.2 Imbalance between Security and Energy Conservation

While working on secure and energy efficient technique it is essential to understand the point where the security is implemented be it a node-based security or routing based security. Majority of the existing studies towards security uses node-based security with less emphasis on routing-based security. However, routing-based security techniques allows authentication scheme in efficient way but posses significant transmission delay. Hence, without focusing on standard radio-based energy model, it is really challenging to ascertain about the effectiveness of security. In reality, majority of the studies discussed in prior Section 2 doesn't use standard radio-based communication model. Therefore, there is much of imbalance between existing security system and energy conservation.

3.1.3 Study Specific to Adversary

It is well known that various forms of adversaries e.g. sinkhole attack, Byzantium attack, node capture attack, blackhole attack, wormhole attack etc. in study of Wireless Sensor Network. Moreover the existing studies on security are much case specific to type of attacker. This will mean that the presented solution is only applicable for one form of attacks. Therefore, it is essential to formulate security system that can understand the forms of attacks and formulate the solution based on the patterns of attack. It was also seen that majority of the adversary node attempt to victimize a node with less residual energy by compromising its authentication system. Hence, fewer studies are witnessed to perform uniform authentication scheme based on public key cryptography.

3.1.4 Lack of Effective Benchmarking

Majority of the existing studies towards security in Wireless Sensor Network are not compared with hierarchical energy efficient routing protocol to prove its energy effectiveness. An effective benchmarking could

be carried out by comparing the presented outcome with both security techniques and energy efficient routing schemes.

The problem statement of the proposed study can be stated as follows – "This is a computationally challenging task to use public key cryptography for ensuring energy-efficient routing technique in Wireless Sensor Network." The next section discusses about proposed system that aimed for overcoming above mentioned issues.

4. Proposed System

Our prior study has focused on discussing existing secure and energy efficient communication system in Wireless Sensor Network[34]. Most recently, we have also presented a technique that uses tree-based technique to secure communication in sensor network[35]. We have also introduced a technique that focuses on robust authentication[36]. Our previous studies are more focused on security and less on energy efficiency. Hence, it was felt that security could be more enhanced with cryptography. However, applying cryptography could also increase the computational complexity and may affect the energy conservation. Hence, we aimed to introduce such a routing technique that incorporates robust authentication technique. We name it as SARDS (Secured Anonymous Routing with Digital Signature). Figure 1 shows the schematic diagram of the SARDS which shows that proposed system has mainly three core module, i.e. 1) A novel lightweight encryption scheme using public key cryptography, 2) A novel digital signature scheme for securing the signing procedure of routing message, and 3) To ensure privacy or anonymity in the routing message. According to SARDS, a sensor node signs the message while performing routing using elliptical curve cryptography. We enhance the flexibility of it by incorporating a novel digital signature scheme as well as discrete anonymity scheme with elliptical curve cryptography. The proposed SARDS scheme uses the similar node-to-node authentication mechanism using the framework of our prior studies. The proposed scheme also introduces a new matrix that stores specific number of arbitrary chosen sensors. Such sensors perform dynamic alterations of the routing information. While performing this operation, SARDS ensure that private information of the communicating sensors never to be disclosed by any sensor whether it may be regular or malicious nodes itself. SARDS provides dual layer of security by using two different forms of mathematical formulations just to generate signature and to authenticate the signatures. The prime objective was to ensure that SARDS use static memory usage while performing security operation along with routing.

The prime contributions of the proposed study are as follows:

- To develop a routing protocol that can maintain a well balance between security and energy effectiveness.
- To develop a routing scheme that allows the message to be encrypted using public key cryptography, this is intended only for destination node.
- To enhance elliptical curve cryptography for simplifying the internal complexity associated with generation and usage of private keys.
- To implement a novel digital signature scheme that can be used for generation of signature and validation of it during the routing operation itself.

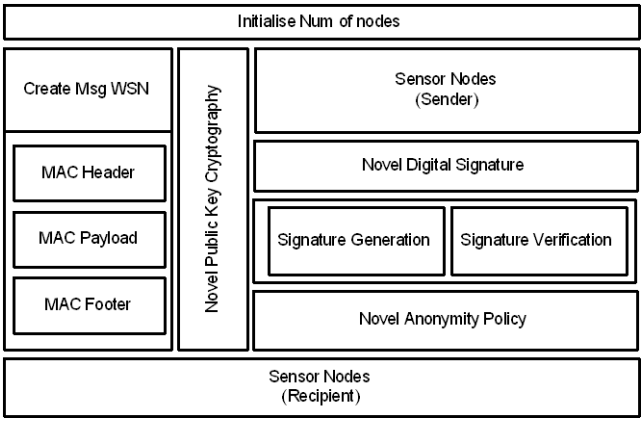

Figure 1. SARDS schema for Wireless Sensor Network.

5. Research Methodology

The proposed study of SARDS uses analytical research methodology for accomplishing the objective of secure routing. Although the prime aim of the SARDS is to accomplish secure communication but the internal architecture of the proposed algorithm also ensures enough energy efficiency at a same time. The basic methodology adopted for designing SARDS is pictorially presented in Figure 2.

It shows a transmitter as well as receiver, which are essentially two cluster heads connected with each other for performing data aggregation. The transmitter

generates a random number, formulate a secret control message along with ciphers and forward the cipher to the next receiving node. However, a receiver node in order to perform deciphering process will require a token or key. In such circumstances, it is quite possible for receiver node to be rogue node and hence it is required to be validated. SARDS performs this task be receiving a validation token from receiver based on which transmitter chooses either to establish routing or to reject any possibility of routing with receiver. This section will further elaborate the prime modules involved in the internal architecture of SARDS as follows:

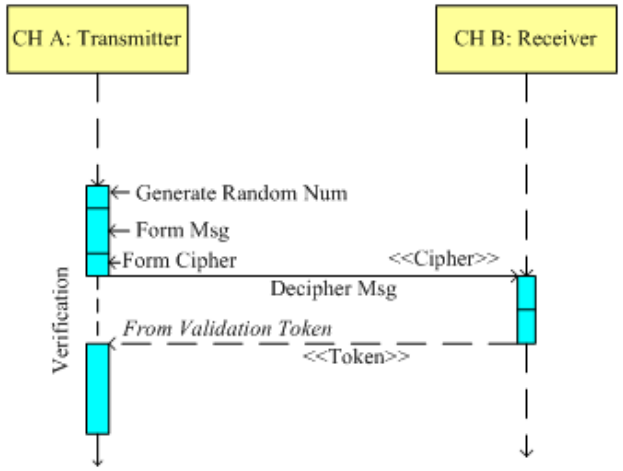

Figure 2. Base methodology of SARDS.

5.1 A Novel Public Key Cryptography

The proposed concept of SARDS uses base of elliptical curve cryptography to use public key cryptography as well as to encode the message such that it reaches only to destination address. Basically, a sensor node starts its communication by broadcasting its beacons, which can be completely compromised by an adversary. An adversary can easily spoof the beacon and make a replica of it to victimize other sensors. Hence, a robust public key can assist in validating the entire communicating node in route discovery and confirmation process. Our technique of is based on finite fields and it utilizes the positional information of the point residing on elliptical curves. One of the best features of elliptical curve cryptography is robust security as well as smaller size of key as compared to frequently adopted RSA algorithm. However, it is also accompanies by issues of complex mathematical designing process that can further shoot computational complexity leading to maximizing the size of the ciphered message even more than encryption using Diffie Hellman and RSA. Hence, we perform some modification towards enhancing the security standards of elliptical curve cryptography. The primary concept of the novel public key cryptography is based on encoding format of the message which could have possible. We consider the message format of the beacon (Figure 3).

Data Frame Format

Octets:2	1	4-20	variable	2
Frame Control	Data Sequence Number	Address information	Data payload	Frame check sequence
MAC header			MAC payload	MAC footer

Acknowledgement Frame Format

Octets:2	1	2
Frame Control	Data Sequence Number	Frame check sequence
MAC header		MAC footer

Figure 3. Message format of Beacon in SARDS.

The above message format shows the presence of simple fields categorized as MAC header, MAC payload and MAC footer. However, the payload is absent in acknowledgement message. Hence, after conversion of the message to binarized encoded format, each message will have unique and different numbers. However, there are possibilities that some of the elements inside binarized encoded message could be found to be repetitive. If such repetitive elements are not repaired that it could lead to discloser of the encoding scheme. Hence, we enhance elliptical curve cryptography to identify such repetitive codes and substitute it appropriate with discrete encrypted codes making it near to impossible for an adversary to decrypt it further. (Figure 4).

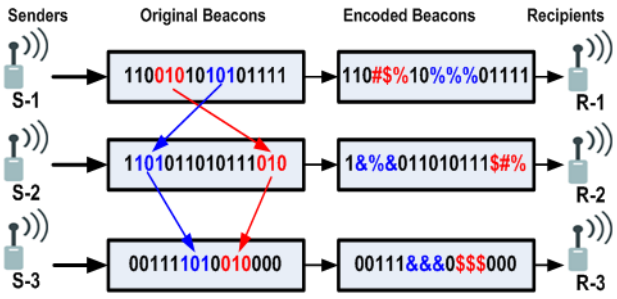

Figure 4. Encoding beacons by enhanced ECC.

Hence, the enhancement done over conventional elliptical curve cryptography are 1) Randomization of third point in elliptical curve, 2) Allows forwarding of unique beacons in every attempt of route discovery as well as for route acknowledgement, 3) Manipulating hashing operation in conventional elliptical curve cryptography with binarized message format to identify repetitive codes. It is further secured using novel digital signature scheme.

5.2 A Novel Digital Signature Scheme

SARDS uses public key cryptography scheme which is based on finite field cryptography over elliptical curves. However, elliptical curves are basically a type of cyclic subgroup in cryptography that leads to a problem of p^k = q where p and q can be denoted as finite group elements. Hence, in order to find the value of k, we use discrete logarithm of it which becomes np hard problem to solve. Usage of various additive, multiplicative, squaring and inversing operation over elliptical curves gives rise to prime fields i.e. generation of private keys. Although the best part of it is to generate reduced numbers of key size but at the same it leads to generation of massive number of key, which may affect computational time. We found that there is no benchmarked technique to solve discrete logarithmic problem in cryptography.

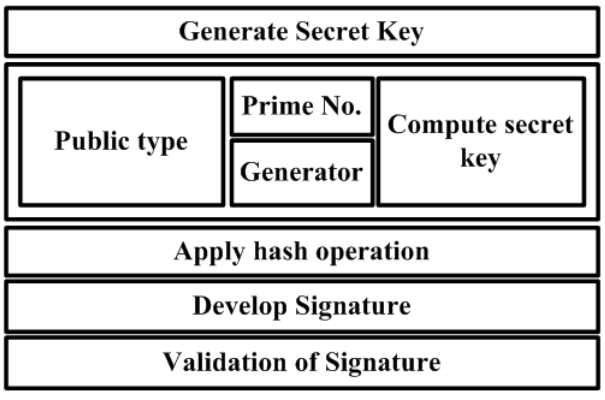

Figure 5. SARDS digital signature scheme.

The novel digital signature scheme consist of mainly three steps, 1) System to generate secret key, 2) Development of Secret key, and 3) Validation of Signature. The system considers α and β to be prime number and secret key generator respectively of the type public. The system then compute the public secret key using k = β^r.mod α. The system then chooses a secret key in arbitrary mode in order to sign the secret message *msg*. The next part of the implementation will be to develop signature as *sig* = enc (γ.r.hash (*msg*, γ)+*l*.mod. (α-1)), where l is another random number. The next phase of the study is to perform validation of the secret signature where we use $\beta^{sig} = \gamma k^{\gamma.hash(msg,\ \gamma)}$.mod α. In case of legitimate signature, the system validates it and allows the system to permit further communication. The variable enc could be any encryption algorithm, however, we use AES.

5.3 A Novel Anonymity Scheme

The proposed SARDS ensure that routing takes place in highly anonymous way where the accessibility of the original message is only for sender and recipient nodes. It doesn't even permit intermediate nodes to access the confidential message by maintaining complete anonymity. The prime intention of this module is to maintain complete privacy. We also consider memory in this regards that will reposit the secure key information (group nodes, certificates, preloaded keys etc). We assume a separate matrix that stores this information inspite of storing the same in nodes thereby saving memory consumption. This matrix is accessed by the nodes that are looking to perform data aggregation. However, we limit this operation for communication between member nodes and cluster heads. Hence, we choose to assume that secret keys (public type) that participate in encryption process will be required to be registered in that matrix. The schematic diagram of the proposed novel anonymity scheme can be seen in the sequence diagram in Figure 6.

The scheme consists of 4 actors e.g. transmitting nodes, matrix of elliptical curve, digital signature and recipient. The sender forwards the message along with the generation of random numbers. The matrix retains all the transactional information e.g. msg, secret keys and then performs encryption which is then forwarded to be signed with the novel digital signature scheme. After the message is received by intermediate nodes, the identity of the originator and destination node address is encoded. We use the primary module to encode the entire control message and distribute the secret keys. This results in subsequent forwarding of the message from one to other node without giving any access rights to any nodes other than the destination nodes. Hence, a perfectly robust and lightweight encryption mechanism is proposed in routing using SARDS.

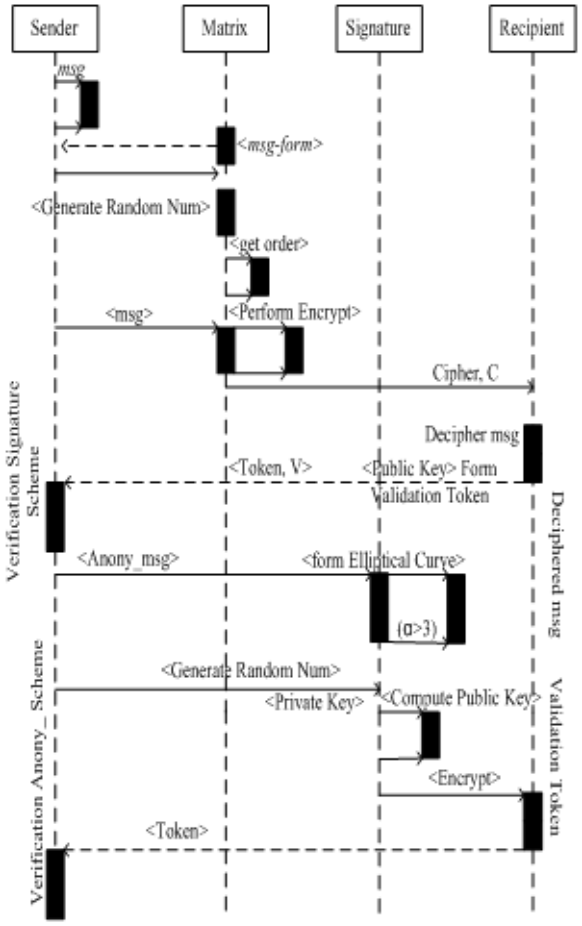

Figure 6. SARDS anonymity scheme.

6. SARDS Algorithm Implementation

The development of the proposed study is carried out using Matlab. The simulation study is carried out for varied number of sensor ranging from 50-500 on both grid and random topology in Wireless Sensor Network. The simulation area considered for SARDS is 1200 x 1500 m^2. The study is also independent from the location of base station. Usually in the area of hierarchical concept of routing, base station normally resides in the center of the simulation area. We discard this concept as positioning base station in center may lead to traffic congestion and at the same time it becomes difficult to perform scheduling of data packets toward base station. Hence, we placed the base station as far as possible from the rest of cluster. This section discusses about the algorithms used for designing proposed SARDS.

6.1 Algorithm for Public Key Cryptography

This algorithm takes the input of the number of nodes (n), transmission area (T_x) of 10 m and a message *msg* of 2000 bytes. The algorithm initially performs computation of two essential points in the elliptical curve i.e. *a* and *b*. It also finds the 2nd point of the elliptical curve q as the base.

Algorithm for Public Key Cryptography

Input: *n* (number of nodes), T_x (Transmission Area), *A* (Simulation Area), *msg* (message).

Output: Encryption of *msg*.

Start

1. init n, T_x, A
2. Eval a, b, prime q
3. Sel(P)→curve
4. Sender(A):→rand(key_i) & Estm key_i*P
5. Sender(B):→rand(key_j) & Estm key_j*P
6. Mat→arb_point(AP)
7. Eval Key_i*Key_j*P*AP
8. Extract Key_{priv} = y
9. Binarize the *msg*
10. If (sim_pat exist among broadcasted *msg*)
12. Encode uniquely
13. Encrypt msg using Key * msg + q mod q
14. Decrypt msg using (step-8)*Key^{-1}+q mod q.

End

The source node A selects an arbitrary secret key key_i that lies between 1 and q. Similar operation is also carried out the other sender node B. Finally, the matrix Mat selects an arbitrary point AP and instantly transmits to both the nodes A and B. Finally, the secret key is computed and then we binaries the msg. If there is a similar pattern *sim_pat* exists among the msg, than we perform discrete encoding to ensure that there is no similar type of encoded message during broadcast. Finally, we encrypt and decrypt the *msg*.

6.2 Algorithm for Digital Signature

This algorithm discusses the usage of encryption standards using asymmetric key. The algorithm considers α as a prime number (odd) that is always greater than 3. Consider that variable a, b and α are the part of original elliptical curve equation ($y^3 = x^3+ax+b \bmod \alpha$). We also consider a reference point acting in base to be F i.e. F = (x_F, y_F). The sender must choose an arbitrary integer whose value must lie within 1 to Z-1 that will be considered as

sender's private key. The sender than computes its public key $key_{pub} = d_A \times F$.

Algorithm for Digital Signature.
Input: msg (message), Z (natural number), s_h (secret share).
Output: generation and validation of signature.
Start
1. arb_{int} = [1, Z-1]
2. $\gamma = r_A$.mod Z
3. if $\gamma = 0$
4. go to 1.
5. hash(*msg*, γ)
6. $s_h = \gamma.d_A.hash_A + key_A$.mod Z
7. if $S_h = 0$
8. go to 2.
9. Generate dig_sig = [γ, s_h]
10. Estimate $hash_A$ & & (r_1, r_2) [$=s_hF - \gamma.hash_A.k_{pub}$]
11. If ($\gamma = r_1$.mod Z)
12. dig_sig = valid
13. or else
14. dig_sig = invalid.
End

The above mentioned algorithm poses essential two steps of operation i.e. generation of signature and validation of signature. An arbitrary integer arb_{int} is selected whose value must lie within 1 and Z-1. Every digital signature must consist of two parts γ and s_h (secret share), which is computed using Line-2 and Line-6. Once the signature pair is generated in Line-9, it is essential to perform validation. Before performing validation, the algorithm checks if keypub is non-zero element or does it is one point inside the elliptical curve or leads to infinity. The validation is performed by authentication γ and sh to be integer type and should lie within 1 and Z-1. The second step is to calculate the hash function of node A and third is to calculate r_1 and r_2 according to Line-10. Therefore, the proposed SARDS perform the authentication of the digital signature without much dependency of network resources and its size on memory consumption is not more than 5-9 bits.

6.3 Algorithm for Anonymity

The prime purpose of the algorithm of anonymity is to ensure that the transmitted routing message proceeds to its destination while maintaining highly privacy factor.

Algorithm for Digital Signature.
Input: *msg* (message), Z (natural number), s_h (secret share).
Output: generation & validation of signature.
Start
1. Select an arbitrary key_i
2. Compute γ_i [(γ_i, k_i) = key_i.F]
3. Select arbitrary key_i
4. Compute γ_t [(γ_t, k_t) = key_t.F-sum ((γ_i, $hash_i$, key_{pub_i})]
5. Estimate $s_h = key_t$ + sum(keyi)+ ($\gamma_t.d_t$, $hash_t$ mod Z)
6. If ((γ_i ki, I = range[0, Z-1])
7. Dig_sig = valid
8. Estimate $hash_i$ (msg, γ_i)
9. Estimate (r_o, k_o) = shF-sum((γ_i, $hash_i$, key_{pub_i})
10. If ic(sum((γ_i, k_i)) = = r_o)
11. Dig_sig = valid
12. Or else,
13. Dig_sig = invalid
End

This algorithm provides dual level of security to the routing message in presence of both internal and external attack in sensor network. The algorithm initially selects an arbitrary key_i in such a way that value of *i* will lie between 1 and Z-1. It is followed by computation of (γ_i), which is very important component of digital signature. However, in order to maintain better level of privacy, we follow here different level of computation for γ_i as compared to previous algorithm of digital signature. Owing to usage of same cryptographic hash function, the memory remains same but elements of the hash matrix keeps on constantly changing. This phenomenon has one big benefit. Even we assume that the message is compromised by an attacker, then also the message is highly secured. As in order to decrypt the message, an attacker will require multiple values of keys which are never possible to be obtained after the message has been already broadcasted by the sender node. Moreover, we perform different formula for calculating secret share s_h which ensures that it is not possible to extract any information from the proposed SARDS digital signature. Our control message will essentially consist of message *msg*, a matrix with legitimate node address *mat*, γ_i, and key_i. Similar principle will be used to perform validation of proposed signature. From the entire message content, the algorithm will only validate γ_i and key_i to ensure if it lies between 1 and Z-1. Hence, SARDS strongly ensure the privacy factor in routing message propagation in Wireless Sensor Network.

7, Results and Discussion

The outcome of the proposed study was compared with the three conventional hierarchical energy efficient routing protocol in Wireless Sensor Network i.e. SecLEACH[37], LEACH[38], and PEGASIS[39]. The study outcomes are as follows:

7.1 Analysis of Energy Efficiency

The outcome of the study shows that proposed SARDS excels much better energy consumption as compared to the existing system (Figure 7). SecLEACH is the only protocol that offers security in comparison to LEACH and PEGASIS. A closer look into the energy curve shows that SecLEACH exhibits energy conservation trend in better than LEACH. However, owing to incorporation of encryption process, the node consumes more energy as compared to PEGASIS. Although, SARDS uses digital signature as well as elliptical curve cryptography, but its operation is restricted to memory allocation of 35 bits, which results in faster processing time and lower energy consumption. We maintain a separate matrix that holds the authenticated information and routing information that also releases the usual load of authentication and message exchange time. This process conserves around 0.27 Joules of energy in each route discovery rounds and conserves around 0.35 Joules of energy in route authentication. Hence, a significant energy is retained in the entire signature generation and verification rounds in simulation study. We also found that with increasing traffic load, SARDS have comparatively lower energy consumption even compared to existing security and energy-efficient routing techniques in sensor network.

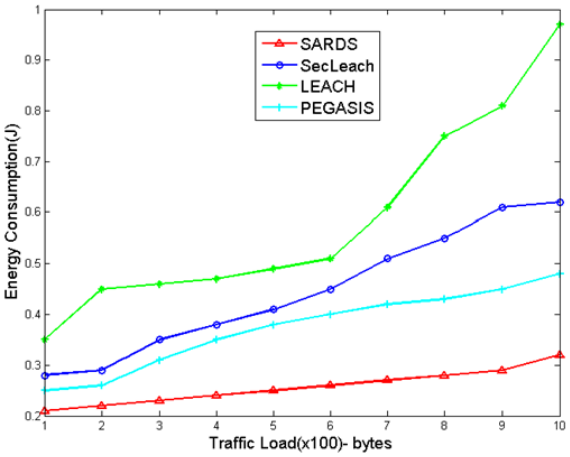

Figure 7. Analysis of energy consumption.

7.2 Anaysis of End-to-End Delay

End-to-end delay is another performance parameter considered for assessing the proposed SARDS. Figure 8 shows that LEACH has considerably increasing delay owing to the position of base station and clustering mechanism. PEGASIS offers reduced delay in comparison to LEACH but misses out security policy within it. SecLEACH performs better than LEACH and PEGASIS; however, SecLEACH has additional overhead owing to direct usage of symmetric key management scheme. This issue is overcome in the SARDS by using combination of public key cryptography and digital signature. The entire authentication scheme takes place faster compared to existing schemes that significantly minimizes the end-to-end delay.

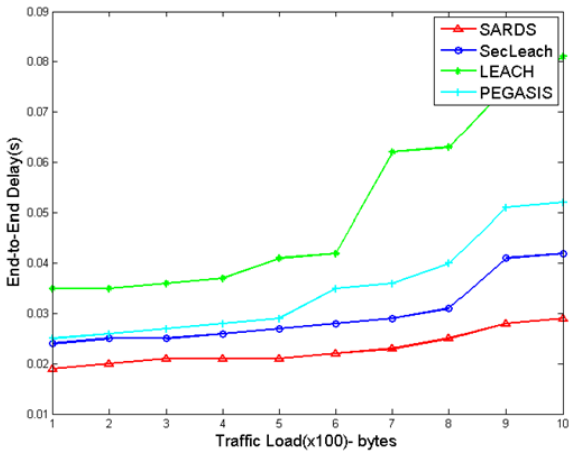

Figure 8. Analysis of end-to-end delay.

7.3 Analysis of Packet Delivery Ratio

Not only this, an evaluation of the packet delivery ratio is conducted on SARDS to check the communication performance. The numerical outcomes are highlighted in Table 1 that shows that SARDS have enhanced packet delivery ratio as compared to existing routing protocol e.g. SecLEACH, LEACH, PEGASIS. We have increased 100-1000 nodes in sequence to understand if traffic load exerted by additional nodes can be catered up properly by nodes. The trends of packet delivery ratio are in decreasing order owing to drainage of energy.

Therefore, the cumulative outcomes shows that SARDS excels better than existing routing protocol both in viewpoint of security but also in communication performance.

Table 1. Numerical analysis of packet delivery ratio

Nodes	SARDS	Sec LEACH	LEACH	PEGASIS
100	0.751	0.624	0.297	0.488
200	0.752	0.62	0.291	0.487
300	0.743	0.613	0.291	0.476
400	0.744	0.611	0.286	0.485
500	0.745	0.562	0.284	0.484
600	0.733	0.562	0.275	0.473
700	0.732	0.558	0.264	0.472
800	0.728	0.543	0.262	0.471
900	0.728	0.544	0.253	0.452
1000	0.777	0.533	0.247	0.451
1100	0.717	0.522	0.244	0.434
1200	0.766	0.515	0.243	0.433
1300	0.654	0.512	0.239	0.427
1400	0.647	0.491	0.236	0.421
1500	0.651	0.488	0.234	0.417
1600	0.651	0.478	0.219	0.399
1700	0.646	0.468	0.216	0.355
1800	0.638	0.465	0.202	0.301
1900	0.616	0.462	0.176	0.287
2000	0.558	0.461	0.1544	0.197

7. Conclusion

This paper discusses about the public key encryption scheme that is mainly meant for dealing with the vulnerable authentication scenario in Wireless Sensor Network. The technique also introduces a technique called as SARDS that offers, 1) A novel public key encryption, 2) A novel digital signature scheme and 3) A novel privacy or anonymous scheme. The total processing time of the SARDS is found to be twice the speed of existing routing techniques discussed in this paper. From performance-based complexity, the system also performs computation of storage complexity by evaluating the length of the message. The interesting point is the proposed system uses a defined matrix to perform authentication based on the total nodes available in the simulation area. Therefore, the proposed system has both lesser processing time and lesser storage complexity. The outcome of the proposed system is also found to be superior as compared to existing protocols e.g. SecLEACH, LEACH and PEGASIS.

8. References

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. Minimum-latency broadcast and data aggregation scheduling in secured Wireless Sensor Network. Springer-Journal. 2015; 9204:550–60.
3. Khan MA. Handbook of research on industrial informatics and manufacturing intelligence: Innovations and solutions. 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 data aggregation. Sensors. 2015; 15(7):15127–58.
5. Das SK, Kant K, Zhang N. Handbook on securing cyber-physical critical infrastructure. Elsevier. Computers; 2012. p. 848.
6. Toghian M, Morogan MC. Suggesting a method to improve encryption 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 encryption 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 using 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 exchange system based on Chinese remainder theorem in heterogeneous wireles sensor networks. Hindawi Publishing Corporation. 2015; 159518: p. 12.
10. Amalarethinam DIG, J. Sai Geetha 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 distributed group key tunneling management protocol for heterogeneous Wireless Sensor Network. Springer-EURASIP Journal onWireless 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 Sensor Network. Springer. 2014; 243:397–408.

15. Liu A, Yang LT, Sakai M, Dong M. Secure and energy-efficient 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 Networkin; 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 Sensor Network. Hindawi Publishing Corporation. EURASIP Journal on Wireless Communications and Networking. 2010.
20. Sheng WX, Zhao ZY, Min WL. Load-balanced secure routing protocol for Wireless Sensor Network Hindawi Publishing Corporation; 2013. 596352. p. 13.
21. Lin H, Ma J, Hu J, Yang K. PA-SHWMP: A Privacy-Aware Secure Hybrid Wireless Mesh Protocol for IEEE 802.11s wireless mesh networks. Springer - EURASIP Journal on Wireless Communications and Networking. 2012 Dec.
22. Fragkiadakis A, Angelakis V, Tragos EZ. Securing cognitive Wireless Sensor Network: A survey. International Journal of Distributed Sensor Networks. 2014, 393248. p. 12.
23. Singh DAAG, Leavline EJ. EERCM: Energy Efficient and Reliable Communication Model for achieving QoS in underwater sensor networks. International Journal of Energy, Information and Communications. 2013 Oct; 4(5):35–44.
24. 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.
25. Ye F, Luo H, Lu S, Zhang L. Statistical en-route filtering of injected false data in sensor networks. IEEE Journal on Selected Areas in Communications. 2015 Apr; 23(4):839–50.
26. Hamid MA, Rashid MO, Hong CS. Routing security in sensor network: Hello flood attack and defense. IEEE ICNEWS; Dhaka. 2006 Jan 2-4. p. 77–81.
27. Lee SH, Lee SJ, Moon KI. A combined system of secure hashing and neural networks in sensor networks of living environment. International Journal of Control and Automation. 2014 Sep; 7(9):55–66.
28. Makvandi N, Hashemi SM, Haghighat P. Detecting attacks in Wireless Sensor Network using genetic algorithms. Proceedings of the International Conference on Computing Technology and Information Management; Dubai, UAE. 2014. p. 374–80.
29. Prasan D, Murugappan. Energy Efficient and Qos Aware Ant Colony Optimization (EQ-ACO) routing protocol for Wireless Sensor Network. International Journal of Distributed and Parallel Systems. 2012 Jan; 3(1):249–56.
30. Rostami A, Mottar MH. Wireless Sensor Network clustering using particles swarm optimization for reducing energy consumption. International Journal of Managing Information Technology. 2014 Nov; 6(4):1–15.
31. Reddy YB. Trust-based approach in Wireless Sensor Network using an agent to each cluster. International Journal of Security, Privacy and Trust Management. 2012 Feb; 1(1):19–36.
32. Kumar RM, Ajitha KS, Ramprasad AV. Reputation based trust management for Wireless Sensor Network and its application to secure routing. International Journal of Innovative Research in Science, Engineering and Technology. 2014 Mar; 3(3):911–5.
33. Shen S, Yue G, Cao Q. A survey of game theory in Wireless Sensor Network security. Journal of Networks. 2011 Mar; 6(3):521–32.
34. Roopashree HR, Kanavalli K. Study of secure and energy efficient hierarchical routing protocols in WSN. International Journal of Engineering Research and Technology. 2014 Jun; 3(6):1221–8.
35. Roopashree HR, Kanavalli A. STREE: A secured tree based routing with energy efficiency in Wireless Sensor Network. IEEE International Conference on Computing and Communications Technologies; Chennai. 2015 Feb 26-27. p. 25–30.
36. Roopashree HR, Kanavalli A. SABR: Secure Authentication-Based Routing in large scale Wireless Sensor Network. Springer - Emerging Research in Computing, Information, Communication and Applications; 2015. p. 223–9.
37. Oliveira LB, Wong HC, Bern M, Dahab R, Loureiro AAF. SecLEACH – A random key distribution solution for securing clustered sensor networks. Proceedings of the Fifth IEEE International Symposium on Network Computing and Applications; 2006 Jul. p. 145–54.
38. Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocols for wireless microsensor networks. Proceedings of the 33rd Hawaaian International Conference on Systems Science (HICSS); 2000 Jan 4-7.
39. Lindsey S, Raghavendra CS. PEGASIS: Power-Efficient Gathering in Sensor Information Systems. IEEE in Aerospace Conference Proceedings; 2002; 3:p. 3-1125–3-1130. Doi: 10.1109/AERO.2002.1035242, 2002.