Integrated Shared Random Key Agreement Protocol for Wireless Sensor Network

Anusha Thanganadar
Department of Computer Science and Engineering,
Anna University, India
anu.cse@psgtech.ac.in

Venkatesan Raman
Department of Computer Science and Engineering,
Anna University, India
prof.r.venkatesan@gmail.com

Abstract: *The secured data transmission in Wireless Sensor Network (WSN) relies on effective key generation and secured sharing. The generated key must be random to enhance data confidentiality. The processes associated with the security in WSN must be designed at reduced computing time and communication cost. Our research work aims to design a novel lightweight key-sharing protocol that is needed for ensuring data confidentiality. The protocol must meet the constraints of WSN by being lightweight and consuming less energy. Security breaches in WSNs occur due to insecure keys. This can be overcome by generating shared keys which are generated once using the dynamic features of Sensor Nodes (SNs) when the Cluster Heads (CHs) are selected. In this research work, we have generated the Master Shared Key (MSK) at the transmitter node by forming a Galois Ring (GR) using WSN parameters and derived the Shared Random Key (SRK) using matched positions of exchanged Random Sequences (RSs). It is protected using a Physically Unclonable Function (PUF). The novelty lies in the SRK generation from MSK which is chosen at random from the polynomials generated during the formation of GR. The MSK is securely shared with the receiver node by encrypting using a Preloaded Key (PK). After this exchange, the key for encryption and decryption is derived by the transmitter and the receiver by exchanging RSs. The SRK is then encrypted using a key which is a unique fingerprint of the SN generated using PUF and stored in the SNs and the CHs to prevent node capture attack that occurs in WSN. Our proposed Shared Random Key Agreement Protocol (SRKAP) is comparable to the Localized Encryption and Authentication Protocol (LEAP) and performs better compared to the Elliptic Curve Diffie Hellman (ECDH) algorithm*.

Keywords: *Energy, entropy, galois ring, sensor nodes, shared random key, physically unclonable function*.

Received August 13, 2023; accepted December 21, 2023
https://doi.org/10.34028/iajit/21/2/3

1. Introduction

Wireless Sensor Networks (WSNs) play a vital role in data collection in IoT systems with limited resources, less battery power, and limited memory usage. Due to the exponential growth of IoT, the scope for the security of data transmitted through wireless devices has increased in the recent past. There is a need for developing lightweight protocols to enhance data confidentiality and it has caught the attention of the researchers Williams *et al*. [33]. The basic idea is to design a simple and energy-efficient key management protocol to be established for a wireless cryptosystem. Securing information assets from intruders is necessary in a network environment [30]. Maintaining the confidentiality of data is required in designing energy-efficient key management protocols. There are two major types of cryptosystems viz., asymmetric key cryptosystem and symmetric key cryptosystem. In an asymmetric key cryptosystem, {public key, private key} pairs are used where Public Key is being broadcasted and Private Key remains secret. In a symmetric key cryptosystem, the secured transmission of data is carried out using session keys during the encryption and decryption of data. Securing the session key is essential for data security in wireless networks since data confidentiality gets lost if it gets caught by adversaries using cryptanalysis.

The backbone of the symmetric key cryptosystem is efficient key generation, distribution, and management. A method for the generation of pseudo-random numbers based on the adaptability of Lattice-based cryptography is proposed Kumar and Mishra [11]. Due to resource and time constraints in WSN, symmetric key cryptosystems are preferred. The simplest method to share secret keys in a WSN is pre-distribution. This is done by loading every node with a set of keys randomly chosen from a large key pool such that two nodes will share one key. While this basic scheme is easy to implement and involves only a little overhead since no costly key agreement must be carried out, it has some disadvantages in terms of scalability and resilience to node capture. Another approach is to involve a Base Station (BS), which can hold a register of secret keys assigned to each node. This mechanism can also be used to authenticate nodes participating in data transmission. In this method, the key distribution could consume energy and the BS could be a bottleneck leading to a single point of failure. Data confidentiality in WSN is achieved by encryption using keys that need to be secured. Key management schemes are categorized as Random key distribution-based schemes, Master key-

based key management schemes, Location-based key management schemes, Tree-based key management schemes, and polynomials-based key management schemes [7].

In the reference paper the researchers Zhu *et al*. [38] proposed a Localized Encryption and Authentication Protocol (LEAP), which uses four kinds of keys for every Sensor Node (SN). It incorporates an individual key imparted to the BS, a pairwise key shared with another node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes. The disadvantages are in terms of the high cost of memory to store the four unique keys for every node when the number of nodes is few. Detection of increased consumption of energy at any cluster helps to detect the presence of malicious nodes in WSN. The usage of light-weight algorithms in WSN increases the lifetime of the mote which paves the way for increased network lifetime.

In our proposed protocol, the Master Shared Key (MSK) gets generated once for each transmitter and receiver, and the Shared Random Key (SRK) gets generated implicitly at the transmitter and the receiver. The generation and sharing of MSK involve computing cost and communication cost while that of SRK involves computing cost only. Energy consumption occurs during the transmission of MSK and the exchange of Random Sequences (RSs) by which the security of WSN is enhanced. The length of the key is variable which adds to the complexity for any adversary to break the key and hence the brute force fails which strengthens the security. MSK is authenticated and sent in an encrypted form. MSK is a linear code whose randomness is tested using National Institute of Standards and Technology (NIST) randomness tests. Both the encrypted MSK and encrypted data are transmitted as WSN data packet frames. SRK gets derived from the decrypted MSK at the receiver and thereby, the data gets decrypted. The randomness of SRK is tested using NIST tests for randomness. SRK is encrypted using the random key generated using the Physically Unclonable Function (PUF) and stored. Since SRK is implicitly shared and stored in another form, SRK remains the shared secret by which the data packets get encrypted. Key gets generated at the SN using PRF by taking Preloaded Key (PK) as input to generate pseudo-random bits. Our proposed protocol is scalable to SRK generation with no performance degradation, the performance of which is compared with LEAP and its variants. The MSK is encrypted using the PK which is device-dependent and unique to SN. Hence the key generated is specific to the transmitter. PK is unique. SRK can be used symmetrically for both encryption and decryption of the data and remains as the shared secret. SRK gets generated from MSK at the transmitter and the receiver implicitly and hence it is protected. The energy behavior of nodes in WSN is presented in Li *et al*. [13] as a "state-event-transition" and proposes an event-driven Queuing Petri-Net (QPN) based modeling technique.

Adding a security component to WSN degrades the performance of WSN by consuming energy at increased computing and communication costs which need to be addressed [28]. Since the security of any cryptographic algorithm lies on an efficient key management protocol, our research focuses on proposing a novel light-weight key agreement protocol at reduced energy consumption, and reduced usage of storage at reduced computing and communication costs. LEAP algorithms are energy-efficient algorithms developed for WSNs at reduced computing and communication costs. Functionalities of different variants of LEAP algorithms viz., LEAP, LEAP+, and LEAP++ are analyzed and an algorithm termed LEAP enhanced [34] is developed for identifying a compromised node in WSN. The paper focuses on incurring extra costs in enhancing security. Among the four different keys used in LEAP algorithms for key management, our paper focuses on the usage of a single shared pair-wise key in WSN overcoming the node capture attack at reduced rekeying overhead. LEAP+ algorithm belongs to the Master key-based key management scheme.

From the research papers that exist in the literature, we found that there is a need to propose a lightweight key agreement protocol that consumes fewer resources and less energy. Also, there is a need to protect SRK from node capture attacks. Accordingly, we have considered the Elliptic Curve Diffie Hellman (ECDH) algorithm as a benchmark and proposed a novel key agreement protocol based on SRK generation securely.

The rest of this research paper is organized as follows: Section 2 describes the basics of WSN and the need for lightweight protocols in WSN. Section 3 discusses the proposed protocol. Section 4 deals with experimental results and discusses the merits of our proposed protocol to LEAP. Section 5 concludes the paper.

2. Literature Survey

Elliptic Curve Cryptography (ECC) is one of the symmetric key cryptographic algorithms [22] in which keys are mutually shared between the nodes in WSN for achieving cryptographic services. WSN is prone to security breaches and hence there is a need to develop lightweight security algorithms for securing WSN. Security is a very challenging task in WSN, the current state-of-the-art security mechanisms are presented in Nesteruk *et al*. [25]. A method for efficient key generation clusters is proposed in Abdullah [1] using the one-way hash function and a random variable for hierarchical WSN clusters to overcome the node compromise attack. This method relies on updating keys by Cluster Heads (CHs) periodically. If CHs fail to update their keys, it is considered a malicious node, even if the nodes are not malicious. Key generation

plays a vital role in security. A method based on polynomial key distribution is being proposed in WSN [3]. Polynomial-based random key generation assures the existence of pair-wise keys between sensors in WSN. The method is prone to node capture attacks which need to be addressed. WSN gets compromised when a fixed number of sensors become compromised. Node capture attack that occurs due to capturing sensitive sequences is overcome to some extent in this proposed method.

A detailed survey regarding key management, authentication, and trust management is done and the need for proposing lightweight protocols for key management is identified. A hybrid encryption algorithm is being proposed in Mehmood *et al*. [19] in which the processes involved in asymmetric key cryptography are reduced with increased inclusion of processes involved in symmetric key cryptography. The work focuses on reducing energy consumption, communication costs, and computing costs with increased security. Security is increased by avoiding node-capture attacks that occur due to the capturing of sequences in our proposed protocol. A two-party Quantum Key Agreement (QKA) with strong fairness property is proposed in Naresh and Reddi [24] and extended to a Multiparty Quantum Key Agreement (MQKA) with strong fairness property withstanding both inner and outer attacks. A comparative analysis was performed with existing techniques. Cryptographic information gets stolen when an SN gets captured by an adversary. An extensive survey of various detection and key pre-distribution schemes used for resilience against node capture attacks is carried out and discussed in Butani *et al*. [5]. The safety period defines the time limit within which the data are maintained safe without being captured by adversaries. The paper presents a security framework with reasonable energy conservation time. The most important attack that needs to be addressed is the node capture attack. It is being overcome by the usage of four different keys at various levels of clustering and also refreshing the keys on demand. A certain amount of energy is consumed during refreshing [9]. A network model that is protected against local, multi-local, and global adversaries that can launch sophisticated passive and active attacks against the WSN is presented in Abuzneid *et al*. [2]. Our research focuses on preventing the node capture attack and conserving energy that occurs due to the refreshing of the keys. Though physical capturing of nodes could not be avoided, node capture attack that occurs due to the capturing of sequences is prevented. Security analysis focuses on whether the WSN functions well without any security breach. Intrusion Detection System (IDS) checks for the existence of malicious nodes through which the information leakage occurs. The usage of machine learning algorithms for detecting malfunctioning WSNs is an active area of research [35]. A lightweight backup and efficient recovery scheme for keys are developed for healthcare which maintains medical records using blockchain technology [36]. A novel intrusion detection scheme based on energy prediction in cluster-based WSNs is proposed in Han *et al*. [8]. Detection of increased consumption of energy at any cluster helps to detect the presence of malicious nodes in WSN. The usage of lightweight algorithms in WSN increases the lifetime of the mote which paves the way for increased network lifetime [12]. Architecture is being proposed in which the message gets encrypted by symmetric encryption and authenticated using a Message Authentication Code (MAC). LEAP algorithms support the usage of four different keys viz., individual key, pair-wise key, cluster key, and global key, among which our research focuses on establishing a pair-wise key that is shared. LEAP algorithms focus on increasing security at minimized energy consumption, communication, and computing costs. Dynamic key management is proposed by using symmetric key cryptography and hash functions. To secure it from attacks, the session key is updated. Key chains are used to prevent node capture attacks [6]. Existing weakness in the Three-factor Light Weight Key Agreement Protocol was proposed in Mo and Chen [21] and analyzed for its security. An extended Euclidean algorithm was used in the generation of secret keys and the method is termed Adequate Sparse Secure and Minkowski distance-based Location Privacy (ASSMLP) [20].

Password-based key agreement protocol has drawn its attention in the cloud for exchanging data [14]. Though it is secure and efficient compared to similar algorithms, it paved the way for the necessity of lightweight algorithms for ensuring data confidentiality at reduced energy consumption, computing cost, and communication cost. Existing key agreement protocols need significant computational requirements and are found to be insecure. Hence an authenticated key agreement protocol between two parties is designed for Vehicle Adhoc Networks (VANET) by generating a secured session key [15]. Analysis of the computational cost and runtime of the existing and proposed algorithms was carried out.

In this paper the researchers Simplicio *et al*. [31] surveyed the various key management mechanisms for distributed sensor networks. The researchers in Philipose and Rajesh [26] investigated energy-efficient sensor node placement in railway systems and found placing the BS at the middle wagon of the train was optimal for data transmission. Also found that there is an increase in energy consumption by 18.51% due to mobility. The researchers in Santos-González *et al*. [27] proposed a secure lightweight password-authenticated key exchange for heterogeneous WSNs. The researchers Keerthika and Shanmuga [10] discuss various active and passive attacks that occur in WSNs and the countermeasures to overcome these attacks.

Our research problem is to propose a novel lightweight protocol at reduced computation and communication costs. It must consume less energy at increased security. The main research problem is to secure the keys used in communicating data over WSN. Also, the most threatening node-capture attack must be addressed. The node-capture attack occurs due to capturing of sensitive sequences in LEAP algorithms and hence there is a need for proposing a novel protocol for overcoming node-capture attacks to some extent. Compared to LEAP algorithms the occurrence of the probability of a node-capture attack is less. ECDH algorithm is a key exchange algorithm that exists in the literature. Hence our proposed Shared Random Key Agreement Protocol (SRKAP) is compared with the ECDH algorithm. The researchers Munilla *et al*. [23] analyzed the shortcomings of symmetric keys based on their availability and proposed a protocol addressing these vulnerability issues supporting forward secrecy. The researchers Attir *et al*. [4] shifted the costly random number generation function from the sensor node to the hub to enhance computation performance, energy consumption, and communication, and the efficiency of the proposed system is evaluated. The researchers Masud *et al*. [18] used PUFs to propose a mutual authentication and secret key establishment protocol by which the doctor's legitimacy and SN were verified before establishing the SK. The researchers Wang *et al*. [32] analyzed the two common security failures namely node capture attack and smart card loss attack. The researchers Shamsoshoara *et al*. [29] surveyed the PUF-based solution for node capture attacks. The researchers in Zheng *et al*. [37] designed an impedance mismatch PUF to generate a unique secret key. The concept of the cryptographic key not being cloned is discussed in the research paper Mall *et al*. [17]. The hardware properties inherent in the devices are mapped to a unique bit stream of information. An authentication and key sharing scheme using PUF, Pedersen's Verifiable Secret Sharing Scheme (Pedersen's VSS), and Shamir's Secret Sharing Scheme (Shamir's SS) are proposed in the research paper Mahalat *et al*. [16]. Based on the papers available in the literature, it is found that there is a need to propose lightweight protocols for the secure transmission of data using symmetric keys. Hence we have proposed a protocol based on Galois Ring (GR) and SRK shared implicitly and protected SRK using PUF generated key.

3. Proposed Protocol

Based on the need for key generation at reduced energy consumption with low computing and communication costs, we have proposed a protocol that satisfies the NIST framework for cryptographic key management.

MSK gets generated using (GR(p,n,r)), where p,n,r are computed from WSN parameters as follows:

- p is the number of ones in the PK.
- n is the sequence number that is retrieved from the frame.
- r is computed from the energy levels of both the transmitter and the receiver.

p^r unique sequences are generated and the randomness of each sequence is tested using NIST randomness tests. One of the RSs is selected for generating MSK from which SRK is derived using generated RSs by the transmitter and the receiver nodes of WSN.

p^r unique sequences are derived using the set,

$$\{1, \varphi, \varphi q\} \tag{1}$$

Where $q=p^{r-2}$, from which an element α is selected randomly and used to form MSK using the coefficients of the following equation:

$$\alpha 0 + \alpha 1 p + \cdots + \alpha n - 1 p n - 1 \tag{2}$$

where each α_i is randomly chosen and belongs to the set.

Sequences of random values are generated by both the transmitter and the receiver nodes and are exchanged. If the generated random values are matched, corresponding bits from MSK are extracted and concatenated to form SRK. The key that is shared between the transmitter and receiver nodes if random can further be used for secured transmission of data. The SRK is encrypted using the random key generated by PUF and its randomness is tested using NIST tests for randomness.

The transmitter can be either SNs or CHs and the receiver can be either CHs or BSs. SRK is generated once from MSK. This process helps in minimizing energy consumption during key generation. SRK remains the shared secret since it gets generated implicitly. Since our proposed protocol is designed for WSN which needs low energy consumption, SRK can itself be used as the key for encrypting the data transmitted and decrypting the data received. Transmitted packets are encrypted and decrypted with SRK using the bitXOR operation. MSK is encrypted with PK using bitXOR and sent to the receiver node. It gets decrypted with the PK of the transmitter node at the receiver using bitXOR operation. PK is piggybacked in the WSN frame packet. The receiver takes the PK from the WSN frame packet and decrypts it. CH generates MSK using GR and transmits it to the SN, after which both SNs and CH generate SRK. Generated SRK is encrypted using PUF and stored in both SN and CH. MSK gets regenerated when the CH changes.

- **Assumptions**

1. CHs are powerful enough to generate MSKs, generate RSs, and receive RSs from all nodes.
2. Each node is equipped with a PUF.

The energy (E) is calculated using,

$$E = V * I * T \tag{3}$$

where,

- *V* denotes voltage.
- *I* denote current.

In our experiment, we have taken *V* as 3 volts and *I* as 19.7mA to calculate the energy consumed in joules.

The flow of operations in our proposed protocol for WSN is illustrated in Figure 1. In this protocol, GR is used for the formation of MSK and the generation of SRK by taking the parameters of SNs as input. The processes involved in the confidential data transmission are illustrated in Figure 2.

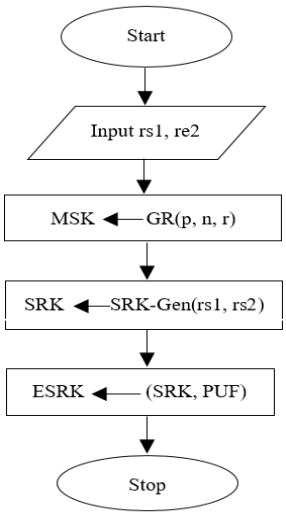

Figure 1. Flowchart for the proposed protocol.

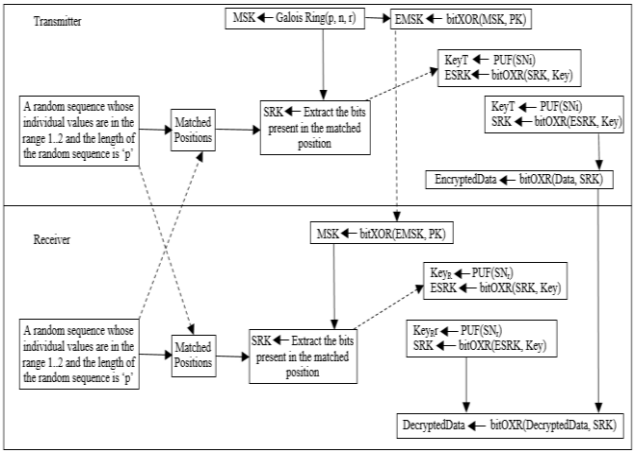

Figure 2. SRK generation for data confidentiality in WSN.

Algorithm (1) explains the formation of MSK using GR by taking p, n, and r as inputs. The epsilon value is calculated by taking p, n, and r as inputs and forming the root_set. A list of root_set is formed. The pterm value is multiplied with a randomly chosen polynomial from the root set. The linked list of the generated polynomials is followed to extract the coefficients. The coefficient in decimal form is converted to a binary number and concatenated to form an RS of bits. Algorithm (2) explains the formation of SRK. Both the transmitter and the receiver nodes generate RSs and the bit from MSK is extracted if the values in the bits in the generated RSs are equal. The protection of generated SRK from node capture attacks using PUF is explained in Algorithm (3). The secured transmission and reception of data in WSN is explained in Algorithms (4) and (5).

Algorithm 1: Master Shared Key Generation Using Galois Ring

Input: p, n, r
Output: MSK
Steps
*1. Form poly1 x^((p*n)^r-1)-1 and poly2←x-1*
2. epsilon←divide_poly(poly1,poly2)
3. root_set[count].coeff←0;root_set[count].pow←0; root_set[count].next←NULL;
4. count←count+1
5. root_set[count].coeff←0; root_set[count].pow←0; root_set[count].next←NULL;
6. For i=2 to 3
count←count+1;
root_set[count].coeff←1; root_set[count].pow←0; root_set[count].next←NULL;
7. For j=1 to i-1
pterm.coeff←pow(p,r);pterm. Pow←0;
root_set[count]←multiply_poly(root_set[count],epsilon);
End For
End For
random_alpha←rand()%size1
8. polynomial←multiply_poly(pterm,root_set[random_alpha])
9. term←polynomial
10. While(temp.next!=NULL)
11. If(temp.coeff>0)
12. MSK←decimal2binary(temp.coeff)
13. temp←temp.next
14. End While

Algorithm 2: Shared Random Key Generation for SRKAP

Input: Master Shared Key MSK, Transmitter Random positions Trandom, Receiver Random Positions Rrandom
Output: Shared Random Key SRK, ESRK
Steps
1. For i←0 to 7
If(Trandom[i]==Rrandom[i])
SRK[count]←MSK[i]
count←count+1
End If
2. SRK[count]← '\0'
3. Output SRK

Algorithm 3: Protecting SRK from Node Capture Attack

Input: SRK, KPUF
Output: ESRK
Steps
For i=0 to length(SRK)
ESRK[i] ← bitXOR(SRK[i],KPUF)
Return ESRK

Algorithm 4: Data Transmission

Input: Data, ESRK, KPUF
Output: SRK, Encrypted Data
For i=0 to length(ESRK)
ESRK[i] ← bitXOR(SRK[i],KPUF[i%8])
For i=0 to length(Data)
EData← bitXOR(Data[i],KPUF[i%8])
Transmit Data

Algorithm 5: Data Reception

Input: EData, ESRK, KPUF

Output SRK, Decrypted Data
Steps
For i=0 to length(ESRK)
ESRK[i] ← bitXOR(SRK[i],KPUF[i%8])
For i=0 to length(EData)
Data← bitXOR(EData[i],KPUF[i%8])
Receive Data

3.1. Secured Hierarchical Key Sharing

Figure 3 illustrates the secured sharing of keys hierarchically in WSN. SRKs are generated by extracting the bit present in the matching bit positions of random sequences between communicating nodes in MSK_{11} shared between CH_1 and SN_{11}.

- SRK_i is generated between BS and CH_i
- SRK_{1j} is generated between CH_1 and SN_{1j}
- SRK_{2k} is generated between CH_2 and SN_{2k}

where i=1, 2, j=1,2 and k=1,2.

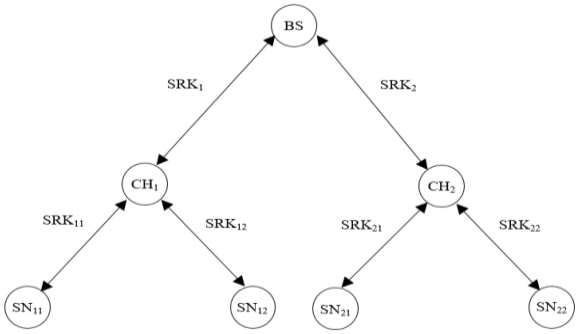

Figure 3. Hierarchical key sharing model.

Figure 4 depicts the generation of SRKs between CH_1 and SN_{11} and their protection using PUF. The generated SRKs are encrypted using the keys KCH_1 and KSN_{11}.

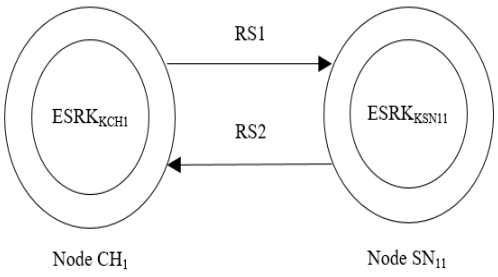

Figure 4. Protecting SRK.

Figure 5 illustrates the steps involved in the generation of SRK and protecting it using PUF. The RSs are Random Sequence 1 which is denoted by RS1, and Random Sequence 2 which is denoted by RS2. SRK_{11} denotes SRK between CH_1 and SN_{11}, KCH_1 denotes the key generated using PUF by taking CH_1 as input, KSN_1 denotes the key generated using PUF by taking SN_1 as input, $ESRK_{KCH1}$ denotes Encrypted Shared Random Key ESRK with key KCH_1 and $ESRK_{KSN1}$ denotes ESRK with key KSN_{11}.

RS1: $SN_{11} \rightarrow CH_1$
RS2: $CH_1 \rightarrow SN_{11}$
$SRK_{12} \leftarrow MSK_{11}$[Matching Positions(RS1,RS2)]
$K_{CH1} \leftarrow PUF(CH_1)$
$ESRK_{KCH1}$<-Encrypt(SRK,K_{CH1})
$ESRK_{KSN11}$<-Encrypt(SRK,K_{KSN11})

Figure 5. Protecting generated SRK using PUF.

4. Experimental Results and Discussion

Energy consumption is directly proportional to execution time. Comparatively, our proposed protocol consumes less energy compared to the ECDH algorithm that exists in the literature.

We infer from Tables 1 and 2 that the time consumption for SRK generation and the energy consumption is less for our proposed protocol compared to ECDH. Time consumption due to random sequence generation by the transmitter and the receiver adds delay for our protocol with increased security.

Table 1. Execution time for SRK generation.

Iteration	Execution time(seconds)		
	ECDH	LEAP	SRKAP
1	1.6e-05	3e-06	4e-06
2	2.2e-05	4e-06	4e-06
3	1.9e-05	3e-06	3e-06
4	2.6e-05	4e-06	3e-06
5	1.7e-05	3e-06	3e-06

Table 2. Energy consumption for SRK generation.

Iteration	Execution consumption(joules)		
	ECDH	LEAP	SRKAP
1	0.00095	0.0001	0.0002
2	0.00130	0.0002	0.0002
3	0.00112	0.0001	0.0001
4	0.00154	0.0002	0.0001
5	0.00100	0.0001	0.0001

Table 3 lists the NIST Tests for randomness. Table 4 lists the generated MSKs and Table 5 lists the generated SRKs.

Table 3. NIST tests for randomness.

Test No.	Test
T1	Frequency test
T2	Frequency block test
T3	Longest runs test
T4	Spectral test
T5	Non-overlapping template matching test
T6	Overlapping template matching test
T7	Approximate entropy test
T8	Binary matrix rank test
T9	Runs test
T10, T11	Serial test

Table 4. List of MSKs.

p	n	r	MSK
7	3	1	MSK1=1111111111101101
7	4	1	MSK2=1001001001001110111101
6	2	1	MSK3=10101010101011
6	5	1	MSK4=10110110110011101100111101
6	6	1	MSK5=110110101100111011010110011101
5	3	1	MSK6=1111111111101101
7	7	1	MSK7=11111010110011101111010110011101

Table 5. List of SRKs.

p	n	R	SRK	ESRK
7	3	1	1111110	0001110
7	4	1	101010111	010010110
6	2	1	10010101011	01110101100
6	5	1	01010111001	10110111110
6	6	1	1111101011011	0001101000111
5	3	1	1111110	0001110
7	7	1	11011111101101	00111111010101

Table 6. p-values of MSK.

Tests	MSK						
	MSK1	MSK2	MSK3	MSK4	MSK5	MSK6	MSK7
T1	1	1	1	1	1	1	1
T2	0.010	0.004	0.017	1.000	1.000	0.010	0.001
T3	0.004	0.004	0.003	0.002	0.001	0.004	0.005
T4	0.000	0.379	0.000	0.006	0.006	0.000	0.000
T5	0.344	0.118	0.344	0.000	0.000	0.344	0.041
T6	0.149	0.124	0.149	0.118	0.118	0.149	0.101
T7	0.005	0.000	0.013	0.125	0.125	0.005	0.000
T8	0	0	0	0	0	0	0
T9	0	0	0	0	0	0	0
T10	1	1	1	1	1	1	1
T11	1	1	1	1	1	1	1
Entropy	0.544	0.994	0.985	0.943	0.940	0.544	0.896
Efficiency	0.546	0.546	0.636	0.5	0.5	0.546	0.636

Table 7. p-values of SRK.

Tests	SRK						
	SRK 1	SRK 2	SRK 3	SRK 4	SRK 5	SRK 6	SRK 7
T1	1	1	1	1	1	1	1
T2	0.050	0.029	0.029	0.029	0.017	0.050	0.017
T3	0.001	0.003	0.003	0.003	0.003	0.001	0.003
T4	0.000	0.000	0.000	0.000	0.000	0.000	0.000
T5	1	1	0.344	0.344	0.344	1	0.344
T6	NaN	NaN	0.149	0.149	0.149	NaN	0.149
T7	0.286	0.131	0.0545	0.055	0.021	0.286	0.013
T8	0	0	0	0	0	0	0
T9	0	0	0	0	0	0	0
T10	1	1	1	1	1	1	1
T11	1	1	1	1	1	1	1
Entropy	0.592	0.918	0.985	0.896	0.779	0.592	0.750
Efficiency	0.546	0.546	0.636	0.636	0.636	0.546	0.636

Tables 6 and 7 show the p-values calculated for MSK and SRK using NIST Tests for randomness. The entropy and efficiency values of the MSKs and SRKs are also tabulated.

The efficiency of the keys MSK and SRK are calculated using,

$$Efficiency = (No.\,of\ tests\ whose\ p-value > 0.01)/11 \quad (4)$$

Sequences with entropy and efficiency values greater than 0.5 are considered random and used as MSKs and SRKs.

Both the ECDH algorithm and the key generation algorithm of our proposed protocol are executed with NS3 installed in 64-bit Ubuntu OS using the processor Intel ® core i5-102100 CPU@1.60GHz x 8. Compared to the ECDH that exists in the literature, our proposed protocol consumes less time and energy.

4.1. Performance Analysis

From Figures 5 and 6, it is inferred that the performance of SRKAP is comparable to LEAP and performs better than the ECDH algorithm.

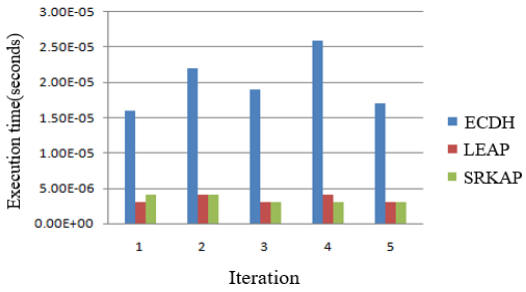

Figure 6. Performance analysis based on execution time.

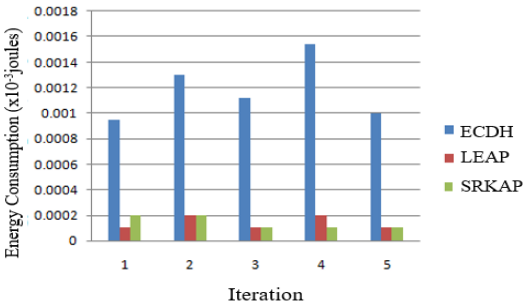

Figure 7. Performance analysis based on energy consumption.

4.2. Security Analysis

- Since the SRK is encrypted using the keys Key_T and Key_R generated using PUF that uses the unique features of a node, the key is protected from node-capture attack by adversaries. The keys Key_T and Key_R are different. An adversary cannot generate Key_T and Key_R. Hence Man-in-the-Middle attacks can be avoided.
- Since SRK can be decrypted only by authenticated entities, impersonation attacks can be avoided.
- Even if MSK is captured since SRK is computed implicitly and protected using PUF, our proposed protocol overcomes the physical attack.
- Data gets transmitted using SRK generated dynamically and hence data transmission is private.

The basic LEAP algorithm is prone to node capture attacks. There exists some time duration within which the node is getting captured in the case of the LEAP+ algorithm. LEAP++ tolerates master key compromise to some extent. LEAP Enhanced identifies the compromised node. Our proposed protocol prevents node capture attack that occurs due to the capturing of exchanged sequences. In LEAP algorithms, the sequence with identified details could be captured by any adversary and hence the node gets captured. It is being avoided in SRKAP since the SRK is implicitly shared. If the sequence about the identity of the transmitter or the receiver is captured by any adversary, transmitting SN or receiving SN gets captured in the case of the LEAP algorithm. In the case of the SRKAP protocol, neither the identity of the transmitter nor the receiver can be captured so the node-capture attack is avoided. Even if an adversary captures MSK, Random Sequence 1, and Random Sequence 2, SRK cannot be generated since the algorithm remains hidden. Random

sequence and MSK travel along with the encrypted packet. MSK and the RSs generated by the transmitter are retrieved from the encrypted packet. The MAC payload field is variable into which the MSK and random sequence can be fitted. The packets are encrypted or decrypted using the SRK computed at the transmitter and the receiver. Sensor data which is of variable length gets fitted into the WSN frame in encrypted form along with the piggybacked MSK. The receiver retrieves MSK. The packet gets decrypted using the SRK computed from the transmitted and received RSs and the MSK.SRK is computed only once by the sender and the receiver to avoid excessive energy consumption. Also, our proposed protocol is scalable and reliable.

When the node is getting captured physically by the intruder only the MSK gets exposed and SRK is protected since it gets implicitly generated dynamically during transmission. Dynamic generation of SRK consumes energy but adds to the security. Since the MSK is generated only once, it contributes to less energy consumption in WSN.

5. Conclusions

Compared to the ECDH algorithm, our proposed protocol consumes less energy and hence supports increased network lifetime. SRKAP suffers from node capture attacks since SRK remains unprotected due to node capture attacks. This drawback is overcome by encrypting SRK with a PUF.

Acknowledgment

We thank the Department of Computer Science and Engineering, PSG College of Technology, Coimbatore, and Centre for Research, Anna University, Chennai for the support given for this research work.

References

[1] Abdullah M., "A Key Distribution and Management Scheme for Hierarchical Wireless Sensor Network," *International Journal of Multimedia and Ubiquitous Engineering*, vol. 6, no. 3, pp. 1-12, 2011. https://www.earticle.net/Article/A153599

[2] Abuzneid A., Sobh T., and Faezipour M., "An Enhanced Communication Protocol for Location Privacy in WSN," *International Journal of Distributed Sensor Networks*, vol. 11, no. 4, 2015. https://doi.org/10.1155/2015/697098

[3] Albakri A., Harn L., Song S., "Hierarchical Key Management Scheme with Probabilistic Security in a Wireless Sensor Network," *Security and Communication Networks*, vol. 2019, pp. 1-11, 2019. https://doi.org/10.1155/2019/3950129

[4] Attir A., Naït-Abdesselam F., and Faraoun K., "Lightweight Anonymous and Mutual Authentication Scheme for Wireless Body Area Networks," *Computer Networks*, vol. 224, pp. 109625, 2023. https://doi.org/10.1016/j.comnet.2023.109625

[5] Butani B., Kumar Shukla P., and Silakar S., "An Exhaustive Survey on Physical Node Capture Attack in WSN," *International Journal of Computer Applications*, vol. 95, no. 3, pp. 32-39, 2014. https://research.ijcaonline.org/volume95/number3/pxc3896265.pdf

[6] Chen C., Chen C., and Li D., "Mobile Device Based Dynamic Key Management Protocols for Wireless Sensor Networks," *Journal of Sensors*, vol. 2015, pp. 1-10, 2015. https://doi.org/10.1155/2015/827546

[7] Gautam A. and Kumar R., "Comprehensive Study on Key Management, Authentication, and Trust Management Techniques in Wireless Sensor Networks," *SN Applied Sciences*, vol. 3, pp. 1-27, 2021.https://link.springer.com/content/pdf/10.1007/s42452-020-04089-9.pdf.

[8] Han G., Jiang J., Shen W., Shu L., and Rodriques J., "IDSEP: A Novel Intrusion Detection Scheme Based on Energy Prediction in Cluster-Based Wireless Sensor Networks," *IET Information Security*, vol. 7, no. 2, pp. 97-105, 2013. https://doi.org/10.1049/iet-ifs.2012.0052.

[9] Jeong G., Seo Y., and Yang H., "Impersonating-Resilient Dynamic Key Management for Large-Scale Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 6, pp. 1-8, 2013. https://doi.org/10.1155/2013/397926

[10] Keerthika M. and Shanmuga D., "Wireless Sensor Networks: Active and Passive Attacks-Vulnerabilities and Countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362-367, 2021. https://doi.org/10.1016/j.gltp.2021.08.045

[11] Kumar A. and Mishra A., "LWE Based Quantum-Resistant Pseudo-Random Number Generator," *The International Arab Journal of Information Technology*, vol. 20, no. 6, pp. 911-918, 2023. https://doi.org/10.34028/iajit/20/6/8

[12] Lara-Nino C., Diaz-Perez A., and Morales-Sandoval M., "Energy and Area Costs of Lightweight Cryptographic Algorithms for Authenticated Encryption in WSN," *Security and Communication Networks*, vol. 2018, pp. 1-14, 2018. https://doi.org/10.1155/2018/5087065

[13] Li J., Zhou H., Zuo D., Hou K., Xie H., and Zhou P., "Energy Consumption Evaluation for Wireless Sensor Network Nodes Based on Queuing Petri Net," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, 2014. https://doi.org/10.1155/2014/262848

[14] Liu P., Shirazi S., Liu W., and Xie Y., "pKAS: A

Secure Password-Based Key Agreement Scheme for the Edge Cloud," *Security and Communication Networks*, vol. 2021, pp. 1-10, 2021. https://doi.org/10.1155/2021/6571700

[15] Li Q., Hsu C., Choo K., and He D., "A Provably Secure and Lightweight Identity-Based Two-Party Authenticated Key Agreement Protocol for Vehicular Ad Hoc Networks," *Security and Communication Networks*, vol. 2019, pp. 1-13, 2019. https://doi.org/10.1155/2019/7871067

[16] Mahalat M., Karmakar D., Mondal A., and Sen B., "PUF Based Secure and Lightweight Authentication and Key Sharing Scheme for Wireless Sensor Network," *ACM Journal on Emerging Technologies in Computing Systems*, vol. 18, no. 1, pp. 1-23, 2021. https://doi.org/10.1145/3466682

[17] Mall P., Amin R., Das A., Leung M., and Choo K., "PUF-Based Authentication and Key Agreement Protocols for IoT, WSN, and Smart Grids: A Comprehensive Survey," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8205-8228, 2022. DOI:10.1109/JIOT.2022.3142084

[18] Masud M., Gaba G., Muhammad G., Gupta B., Kumar P., and Ghoneim A., "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," *IEEE Internet of Things Journal*, vol. 8, no. 21, 2021. DOI:10.1109/JIOT.2020.3047662

[19] Mehmood G., Khan M., Waheed A., Zareei M., Fayaz M., Sadad T., Kama N., and Azmi A., "An Efficient and Secure Session Key Management Scheme in Wireless Sensor Network," *Complexity*, vol. 2021, pp. 1-10, 2021. https://doi.org/10.1155/2021/6577492

[20] Meena U. and Sharma A., "Adequate Sparse Secure and Minkowski Distance Based Location Privacy Approach in Wireless Sensor Network," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 3, pp. 280-289, 2017. DOI:10.22266/ijies2017.0630.32.

[21] Mo J. and Chen H., "A Lightweight Secure User Authentication and Key Agreement Protocol for Wireless Sensor Networks," *Security and Communication Networks*, vol. 2019, pp. 1-17, 2019. https://doi.org/10.1155/2019/2136506

[22] Moon A., Iqbal U., and Mohiuddin Bhat G., "Authenticated Key Exchange Protocol for Wireless Sensor Networks," *International Journal of Applied Engineering Research*, vol. 11, no. 6, pp. 4280-4287, 2016. https://api.semanticscholar.org/CorpusID:40021041.

[23] Munilla J., Burmester M., and Barco R., "An Enhanced Symmetric-Key Based 5G-AKA Protocol," *Computer Networks*, vol. 198, pp. 108373, 2021. https://doi.org/10.1016/j.comnet.2021.108373

[24] Naresh V. and Reddi S., "Multiparty Quantum Key Agreement with Strong Fairness Property," *Computer Systems Science and Engineering*, vol. 35, no. 6, pp. 457-465, 2020. https://doi.org/10.32604/csse.2020.35.457

[25] Nesteruk S., Kovalenko V., and Bezzateev S., "A Survey on Localized Authentication Protocols for Wireless Sensor Networks," *in Proceedings of the Wave Electronics and its Application in Information and Telecommunication Systems*, Petersburg, pp. 1-7, 2018. DOI: 10.1109/WECONF.2018.8604433

[26] Philipose A. and Rajesh A., "Investigation on Energy Efficient Sensor Node Placement in Railway Systems," *Engineering Science and Technology, an International Journal*, vol. 19, no. 2, pp. 754-768, 2016. https://doi.org/10.1016/j.jestch.2015.10.009

[27] Santos-González I., Rivero-García A., Burmester M., Munilla J., and Caballero-Gil P., "Secure Lightweight Password-Authenticated Key Exchange for Heterogeneous Wireless Sensor Networks," *Information Systems*, vol. 88, pp. 101423, 2020. https://doi.org/10.1016/j.is.2019.101423

[28] Sen J., "A Survey on Wireless Sensor Network Security," *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, pp. 55-78, 2009. https://arxiv.org/ftp/arxiv/papers/1011/1011.1529.pdf

[29] Shamsoshoara A., Korenda A., Afgahah F., and Zeadally S., "A Survey on Physical Unclonable Function (PUF)-Based Security Solutions for the Internet of Things," *Computer Networks*, vol. 183, pp. 107593, 2020. https://doi.org/10.1016/j.comnet.2020.107593

[30] Sharifi A., Zad F., Farokhmanesh F., Noorollahi A., and Sharifi J., "An Overview of Intrusion Detection and Prevention Systems (IDPS) and Security Issues," *IOSR Journal of Computer Engineering*, vol. 16, no. 1, pp. 47-52, 2014. https://www.slideshare.net/IOSR/h016114752?next_slideshow=true

[31] Simplicio M., Barreto P., Margi C., and Carnello T., "A Survey on Key Management Mechanisms for Distributed Wireless Sensor Networks," *Computer Networks*, vol. 54, no. 15, pp. 2591-2612, 2010. https://doi.org/10.1016/j.comnet.2010.04.010

[32] Wang C., Wang D., Tu Y., Xu G., and Wang H., "Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 507-523, 2022. DOI:10.1109/TDSC.2020.2974220

[33] Williams P., Dutta I., Daoud H., and Bayoumi M., "A Survey on Security in the Internet of Things with a Focus on the Impact of Emerging Technologies," *Internet of Things*, vol. 19, pp.

100564, 2022. https://doi.org/10.1016/j.iot.2022.100564

[34] Yassine M. and Ezzati A., "LEAP Enhanced: A Lightweight Symmetric Cryptography Scheme for Identifying Compromised Node in WSN," *International Journal of Mobile Computing and Multimedia Communications*, vol.7, no. 3, pp. 42-66, 2016. DOI:10.4018/IJMCMC.2016070104

[35] Zahednejad B., Ke L., and Li J., "A Novel Machine Learning-Based Approach for Security Analysis of Authentication and Key Agreement Protocols," *Security and Communication Networks*, vol. 2020, pp. 1-15, 2020. https://doi.org/10.1155/2020/8848389

[36] Zhao H., Bai P., Peng Y., and Xu R., "Efficient Key Management Scheme for Health Block Chain," *CAAI Transaction on Intelligence Technology*, vol. 3, no. 2, pp. 114-118, 2018. https://doi.org/10.1049/trit.2018.0014

[37] Zheng X., Zhang Y., Zhang J., and Hu W., "Design Impedance Mismatch Physical Unclonable Functions for IoT Security," *Active and Passive Electronic Components*, vol. 2017, pp. 1-8, 2017. https://doi.org/10.1155/2017/4070589

[38] Zhu S., Setia S., and Jojodia S., "LEAP+: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 4, pp. 500-528, 2006. https://doi.org/10.1145/1218556.1218559

Anusha Thanganadar received her B.E degree in 2002 in Computer Science and Engineering from Dr. Sivanthi Aditanar College of Engineering, Tiruchendur, and her M.E degree in Computer Science and Engineering in 2009 from Manonmaniam Sundaranar University, Tirunelveli. She is designated as Assistant Professor (Sel. Grade) in the Department of Computer Science and Engineering, PSG College of Technology, Coimbatore, Tamil Nadu, India.

Venkatesan Raman received his B.E. (Hons) degree from Madras University in 1980. He completed his Master's degree in Industrial Engineering from Madras University in 1982. He obtained his second master's degree MS in Computer and Information Science from the University of Michigan, USA in 1999. He was awarded with Ph.D. from Anna University, Chennai in 2007. He is designated as a Professor in the Department of Computer Science and Engineering, PSG College of Technology, Coimbatore, Tamil Nadu, India.