Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Novel secret sharing scheme based on key transfer protocols in a wireless sensor network environment

Muhammad Sulaiman Khan [1, *], Farhan Ali [1, 2], Wang Wei [1], Na Xia [1], Nadeem Khan [1]

[1]Department of Computer Science and Information Technology, Hefei University of Technology, Hefei, China
[2]School of Electrical Engineering and Automation, Hefei University of Technology, Hefei, China

ARTICLE INFO

Article history:
Received 19 October 2019
Received in revised form
4 March 2020
Accepted 7 March 2020

Keywords:
Secret sharing scheme (SSS)
Cryptographic protocols
Wireless sensor networks (WSNs)
Sensor systems
Linear algebra
Computer networks

ABSTRACT

Wireless sensor network (WSN) application is an emerging industry in the field of computer technology. WSN application plays a commercial role in different domains, such as military surveillance targeting, area monitoring, health care monitoring, environmental sensing, and data center monitoring. However, these applications face various problems, such as the lack of security protocols within devices as well as data transmission and communication issues in between sensors. That's why, in the current age, security is the focus of many works, and constructing powerful security protocols is very challenging. Researchers currently focus on user's confidentiality in WSNs environments to analyze problems using various approaches, claiming data security is the most salient concern for unauthorized entities. So, A WSN is a superior type of communication network because it shares data in special manners during the deployment of sensor nodes. Certain characteristics are unique to it. Secret sharing scheme is one of the most innovative and powerful schemes in the modern era of the cryptographic world, which consists of two basic parts, namely, distribution and reconstruction Unceremoniously, Secret Sharing Scheme is working on a unique player called dealer which contains the smallest size of every participant shared secret information. It is a very significant aspect when they distribute the secret, and it would be a small size of the share as needed for the energy-constrained WSNs under the comprehensive security application. Therefore, we presented a theoretically secure, novel secret sharing scheme (SSS) for WSN applications, especially for key transfer protocol.

1. Introduction

In this modern era, wireless sensor network (WSN) applications play a vital role in different domains, such as information technology, electronics, healthcare, and hazardous environments. These applications aim to obtain information from different fields. In these applications, data security is the most salient concern for unauthorized entities. A huge amount of graphic data, such as images and videos, could be composed of sensor nodes (Liu et al., 2018). These data are mostly authorized by the approachability of sensors that are too small, inexpensive, and with limited memory storage and computational power, but they also perform very intelligently (Pottie and Kaiser, 2000; He et al., 2016). In general, collected data from the sensor nodes could be transferred and combined from the gateway node occasionally. However, if users intend to access the total amount of data from the sensor getaway node, then they must be authenticated first to the getaway node. Users need to access the data from the nodes directly in certain applications, such as healthcare observing, battlefield surveillance. Data is the most important factor in sensor nodes, and sensors are highly sensitive and discreet. Therefore, an authentication policy between a user and a senor is necessary. To date, many authentication schemes are proposed (Das, 2009; He et al., 2010; 2015a; Khan and Alghathbar, 2010; Sun et al., 2013; Watro et al., 2004; Xue et al., 2013; Yeh et al., 2011) in this scenario. Moreover, getaway must be authenticated, and the user must be classified as real or fake. In the case of a real user, a common session key shall be created between the user and sensor node with the

* Corresponding Author.
Email Address: 2016111384@mail.hfut.edu.cn (M. S. Khan)
https://doi.org/10.21833/ijaas.2020.06.004
Corresponding author's ORCID profile:
https://orcid.org/0000-0003-0429-8812

support of the getaway sensor node. After this scenario, the session key will be used for the protection and integrity of the required data (Shen et al., 2017a). Introducing cryptographic schemes over WSNs at different secure applications is a highly challenging condition for researchers and scientists. Moreover, wired networks have very high bandwidth capacity and working power. Hence, WSNs are unique technology with unique features (Wood and Stankovic, 2002). WSNs have very important features, such as group key management, ensured confidentiality, robustness in contradiction of communication, denial of service attack, and verification. Moreover, these applications may contain authentication in group-based management, intrusion, and detection as well as security against traffic flow examination. Encryption and decryption techniques are commonly used for protecting group-based communication. The keys must be handled in a secure way when they are undergoing updating, creating, analyzing, and distribution to ensure the security of group-based communication. Moreover, the key establishment protocol prior to altering secret data is to share the keys across all within-group participants in a very secure way. The main key establishment protocols used are key transfer and key agreement protocols. Key transfer protocol (KTP) depends on the key generation center (KGC), which chooses the group key for communication among group members by distributing one or more keys during registration. With respect to the key agreement protocol, the common group key is resolved by interchanging the public keys of two communication parties in the presence of communication entities. Authenticated group communication (AGC) is the process in which members of a group can communicate in a very secret manner, and the group information is not accessible to any person outside the group. In this situation, a group key is created for each participants' group members. Such a key could be used to encrypt all the messages intended for the group.

Secret sharing has been used for creating "group key distribution protocols" in recent years. Two main types of "group key distribution protocols" are considered in this study. We assume one trusted offline server that can be active only at initialization (Sáez, 2003); an active server always active sees details (Laih et al., 1989). The first type of protocol is called the key pre-distribution scheme, wherein a trusted server, that is, KGC, creates and distributes small pieces of information to all the trustee's offline users. When starting group communication, each legal group member can compute the secret key of the group, whereas illegal members cannot access the key. A substantial disadvantage in this approach is that each user involved in communication must store substantial secret information. In the second type of approach, an online server must be active and can distribute group keys to every member of the group. Secret sharing is used for different protocols of WSNs, including group key management, and data confidentiality is required (Harn and Lin, 2010; Lee et al., 2011; Di Pietro and Guarino, 2013). Authenticated group key transfer protocol (AGKTP) introduced in Harn and Lin (2010) requires an online key generation center for constructing and distributing a group-based key. These keys raise the overhead to construct the system while decreasing the system's flexibility. A method for replicating the keying scheme is explored in Lee et al., (2011), and this method is more active without a trusted server called KGC. In this regard, a group key created is between the trusted members and all the group members for the final key derivate. However, both schemes (Harn and Lin, 2010; Lee et al., 2011) cover coupling-based computations, which cannot deliver the cipher group for universally attached to WSN devices. Similarly, these schemes have security weaknesses as verified in Yuan et al. (2013); these weaknesses include doubt of chasing the random values for every member in group and doubt on man in the middle attacks. This article is organized as follows. Section 2 features related works regarding the proposed scheme, section 3. Security challenges for WSNs, Section 4 reviews different types of attacks on WSNs. Sections 5, 6, and 7 present the proposed schemes, discussions, and conclusions of the article.

2. Related work

In the case of the security features under the aforementioned applications, many secure protocols have been proposed (Shen et al., 2017b; He et al., 2015b; Jiang et al., 2017; 2018). Researchers currently focus on user's confidentiality in WSNs environments. Different researchers analyze problems using various approaches, claiming security in their proposed protocols. We studied the following proposed protocols. Shamir (1979) proposed a very basic scheme on how to divide secret information $S = s_1, s_2, s_3, \ldots . s_n$ participants and presented a concept for reconstruction of shares. Their scheme is suitable for key management in cryptographic devices. Kurihara et al. (2008) proposed a new scheme based on (k, n) threshold scheme. This scheme gives the concept of high performance. The researchers used the basic concepts of EXCLUSIVE-OR functions for recovery the secret information. Omote and Thao (2015) proposed the concept of a secret sharing scheme (SSS), which is based on sleeping wolf coding. They tried to obtain an optimum size of shares as well as renew the shares deprived of identifying secret. Koga and Honjo (2014) examined an SSS that is based on shortened Reed–Solomon code. They divided L secret information $s_1, s_2, s_3, \ldots . s_l$ in between the n shares of participants $t_1, t_2, t_3, \ldots . t_n$ to satisfy certain $n - k + l$ system of linear equation. Hsu et al. (2016) designed a protocol based on linear SSS, an assumption of factoring problem. This scheme is suitable for special WSN applications, such as key transfer protocols. Hsu et al. (2014a)

constructed a key transfer protocol based on SSS for big data problems. This protocol works without an online position of KGC. The researchers used a DH key agreement via key encryption and decryption. Hsu et al. (2014b) proposed an authenticated protocol, which is based on LSSS as well as the EI Gamal cryptosystem. KGC can send secret key information to each participant members. The researchers claimed that transferred keys within the protocol must be secured. Sun et al. (2012) used an enhanced SSS that is deprived of Langrage interpolation polynomial. They proposed a scheme based on mutual authentication for a surety, wherein participants within the group could achieve only the accurate session key. Moreover, all members could store only a unique secret key for each session during the communication flow. Changes in any group member will not affect existing shares. Jaiswal and Tripathi (2017) introduced a novel based group key transfer protocol by implementing elliptic curve cryptography (ECC) as well as Shamir (1979) SSS. In this protocol, any group member could play the role of KGC without online condition. Harn et al. (2018) proposed protocol, wherein they escaped the mutually trusted server KGC, and each user played an active role as a trusted user. During the initialization phase of registration, each user plays an active role as a KGC to give access to another user and provide sub shares to other members. Homomorphism SSS enabled each sub share of every member to be joint in a master share. Moreover, the master share could publish a pair-wised key in between the pair of members. Eschenauer and Gligor (2002) proposed key management schemes for design to gratify the operational and authentication requirements of WSNs. In their schemes, they chose the distribution and cancelation of keys to direct sensor nodes and node rekeying that are deprived of computation and communication competencies. Their research approach was scalable and flexible, and adjustment could be built between senor memory and connectivity. In the solution of the scheme, every sensor would be initialized within a ring key.

Chan et al. (2003) proposed a protocol called "q-composite scheme," which features flexibility and random key scheme (RKS). RKS is a fundamental solution based on a couple of nodes that create a protected path when they distribute q-keys. Moreover, they found a solution to node detection attacks because the adversary required intersection keys to break an authenticated link. This solution damages the system over a network regarding authenticated connectivity. Rasheed and Mahapatra (2011) proposed a couple of key pre-distribution scheme, which permits a mobile sink to create a secure data communication channel regarding sensor nodes. This scheme is basically based on the polynomial-based pool scheme. The security of this scheme indicates, with high probability and short communication cost, that a sensor node could create pairwise keys among the mobile sink. Ruj et al. (2013) designed a pairwise key scheme for WSN in the utilization of pre-distribution based on combinational design. The benefits of this scheme over pairwise keys are security and bandwidth necessities, which are eligible for stationary and mobile service networks. They applied a polynomial scheme for each of the three nodes in case of a unique key. Li and Xiong (2013) proposed an online and offline sign-cryption-based scheme, which permits a sensor node in identity-based cryptography to deliver a message to an Internet host regarding PKI. The scheme could reduce the computational cost for sensor nodes. The researchers claim that the scheme is suitable for WSNs and IoT solutions. Blom (1983) proposed an establishment scheme for pairwise keys grounded on threshold cryptography. Zhang et al. (2018) proposed a key exchange protocol based on ECC. This protocol is suitable for WSN applications. However, it consumes higher energy than computation resources. Khan et al. (2012) introduced a key establishment protocol for WSNs using a pre-distribution scheme with the help of a symmetric matrix regarding maximum rank distance. They divided sensor nodes into multiple groups, and they took part in information in each node of senor to create link keys between all nodes. Wu et al. (2017) proposed an authenticated scheme, which will be secure in the formal model as regard security purposes. Watro et al. (2004) introduced a scheme based on the RSA algorithm in the sensor environment. Das (2009) proposed a two-factor authenticated scheme for WSNs. However, certain researchers (He et al., 2010; Khan and Alghathbar, 2010) found a weakness in the Das (2009) proposed protocol. A brief introduction on different types of attacks on WSNs

Most WSN protocols are too simple and weak against different types of attacks, which work on ad hoc networks. Many threats in WSNs occur during communication over the networks. We discuss some of the attacks as follows:

1. Spoofed/altered attack: This type of attack can target data of routing swapped in between the node. The attacker can create a routing ring that can produce wrong information, such as large end-to-end inactivity, decreased source gateways, and network barrier.
2. Selective forwarding attack: This type of attack, malicious nodes, could decline because of specific onward information, and they fundamentally fall down. A malicious node could not spread ahead, and it could behave like a black hole. Moreover, each established message could be rejected. This type of attack is fast and efficient because the attacker could involve the data flow between the different nodes.
3. Sinkhole: In this type of attack adversary, a sinkhole must be established at the midpoint. An attacker always tries to obtain data flow in a certain path to compromise node regarding particular routing algorithms. Action nodes will be compromised and affect side nodes. Many

protocols could try to examine the quality between end-to-end sessions and encompassing the reliability of the messages.

4. Sybil attack: As regards this attack, one node tries to offer multiple individualities to an against node over the network. It could be meaningfully decreased and affect the failure of the network. This type of attack is placed in different places at once.
5. Wormholes attack: In such a kind of attack, an attacker could be a single part of the network and can catch messages over the dormancy path and pay them back in between different parts over a tunnel.
6. HELLO flood attack: This very high type of attack is presented by a sensor network. Here, a node could be persuaded by such an adversary to be loyal for being a nearby member and having the ability to transfer the wrong information with the high-speed flow.
7. Spoofing attack: The objective of this attack is that an attacker can try to prove a sender-side that a dead node is strong or a weak path is strong. An adversary can remove messages flow against the dead nodes (Ali et al., 2019a; 2019b).

3. Security challenges for WSNs

A WSN is a superior type of communication network because it shares data in special manners during the deployment of sensor nodes. Certain characteristics are unique to it. Security for WSNs services can defend the data communications with the support of unique keys over the network, and attackers could mislead the nodes of data. Certain important security needs are listed under the following:

1. Data privacy: The security appliance could guarantee that no message within the network is analyzed by the attacker, except the participant. The two most important issues exist concern privacy in WSNs. The sensor node could not permit its reading to be retrieved by its neighbors, except they are authorized. The mechanism of key transfer should be robust. Public data suppose for sensor characteristics. Public keys for sensor nodes could be encrypted by actual conditions for the protection against attackers.
2. Availability: This section ensures that facilities for WSNs must be in the present condition. Even the availability of attacks supposes as DOS-denial of service. Scientists and researchers propose different types of schemes.
3. Authentication: It allows required sources or close-fitting information to authenticate by sensor nodes from base to heads stations.
4. Authorization: As regard authorization, only legal nodes could negotiate a special activity.
5. Freshness: It defines whether the data is fresh and can provide a security layer over the network in regard to attack.
6. Integrity: No entity and message could be altered, and it tries to negotiate between sender to receiver.

Cryptography secured schemes are mostly used to support the basic requirement of sensors networks. However, the sensor nodes are very sensitive in the case due to computational and memory capabilities. The most popular traditional techniques of cryptography could not be simplified to move in WSNs without familiarizing them. Two basic keys, namely symmetric and asymmetric keys, are used in WSNs for security purposes.

3.1. Symmetric key

A symmetric key is also called secret-key cryptography. This key allows the use of a single key for encryption and decryption purposes. This key is used as a secret over a WSN, making it very hard to expose. This key is more efficient than the asymmetric key system. The process is not complicated when applying encryption and decryption methods, such as AES and 3DES. Fig. 1 shows the encryption and decryption processes in the symmetric key.

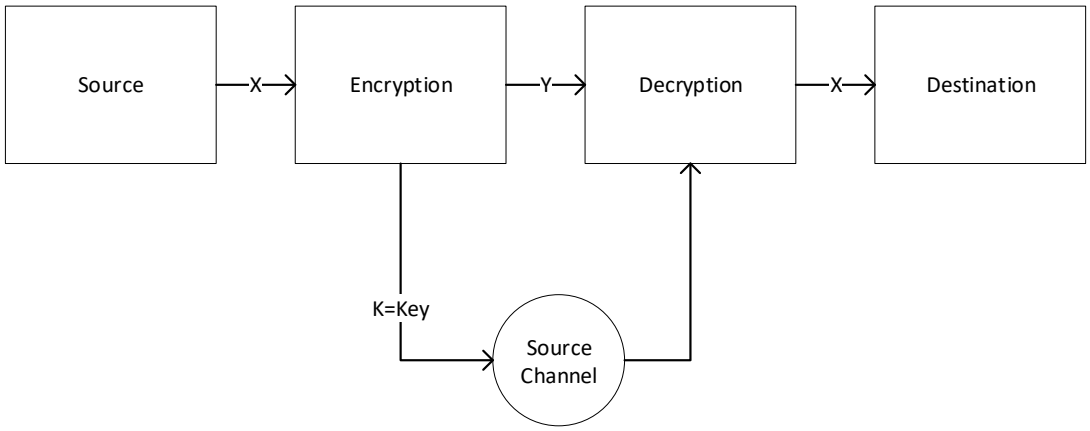

Fig. 1: Symmetric key process

3.2. Asymmetric key

We can also call public key cryptography. This technique enables us to use two kinds of keys, that is, public and private, for the case of encryption and decryption process data over networks. In this technique, a private key cannot be compromised. In such a process, a message could be encrypted by a public key and will be decrypted by using the same kind of algorithm to compare with the private key, as shown in Fig. 2. Such examples are RSA and ECC. For additional details of these algorithms, see Fig. 1. Table 1 shows cryptography algorithms.

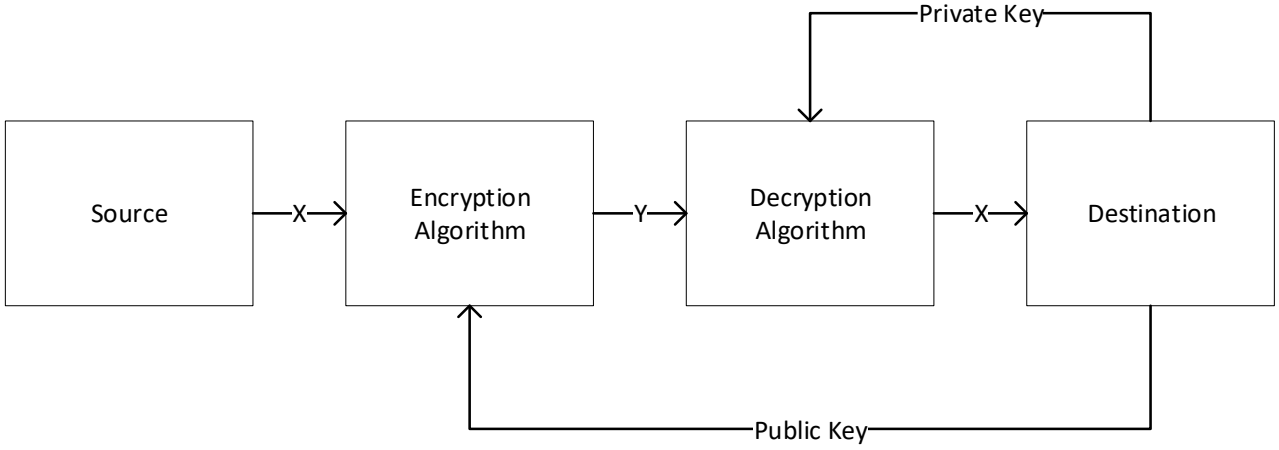

Fig. 2: Asymmetric key process

Table 1: Cryptography algorithms

Algorithm Parameters	Algorithm Domain				
	Public Key Cryptography				
	DES (Davis, 1978)	3DES (Barker and Barker, 2008)	Blowfish (Schneier, 1994)	ECC (Miller, 1986)	AES (NIST, 2001)
Keys Used	Same Key used for encryption and decryption	Same Key used for encryption and decryption	Same Key used for encryption and decryption	Same Key based on algebraic structure of elliptic curve	Same Key used for encryption and decryption
Nature of Algorithm	Feistel Structure	Feistel Structure	Feistel Structure	Algebraic Structure	Feistel Structure
Tunability	No	Yes	Yes	Yes	Yes
Rounds	16	48	16	1	10, 12, 14
Encryption Ratio	High	Moderate	High	High	High
Throughput	Lower than ES	Lower than DES	Very High	Low	Lower than Blowfish
Environment based Modification Support	No, DES does not support any modification	The keys size id increased from 56 to 168 bits	Key length in blowfish should be multiplies of 32	No Modification in key length Linearly increase as security level increases	128, 192 or 256 its structure was flexible to multiplies of 64
Cloud Compatibility	Yes (not used, easy to break and prone to many attacks)	Yes (not used, easy to break and prone to many attacks)	Yes, mozy breakup, Foopchat, Gigatibe	Yes, Microsoft Azure web services	Yes, Google Drive, OneDrive, Dropbox
Application	Smart Card	Microsoft OneNote, Outlook 2007	IDS server, SQL server 2000	Web-Based SSL Protocols like HTTP, IPsec	Password Manager
Proved Security against	Brute Force Attack	Brute Force, Chosen Plain	Dictionary Attacks	Side-channel attack	Chosen Plain, Known Plain

Novel-based proposed schemes

4. Secret sharing scheme

SSS is one of the most innovative and powerful schemes in the modern era of the cryptographic world, as mentioned in the literature (Shamir, 1979; Blakley, 1979; Blum, 1983). In general, SSS consists of two basic parts, namely, distribution and reconstruction. Unceremoniously, as regard (m, n) SSS, this scheme working on very unique player called a "dealer."

A dealer must distribute the secret information s in between of n participants, such as $P_1, P_2, P_3, \ldots . P_n$. The dealer could send a share in among of every player, which is indicated as s_i to p_i of the secret information s in such a manner that any member of group m or up more players can recover the secret collect in the sense of togetherness. However, no group of fewer than m players could do it. Here, we can see the process of share distribution and reconstruction. Fig. 3 shows the share distribution/reconstruction phase.

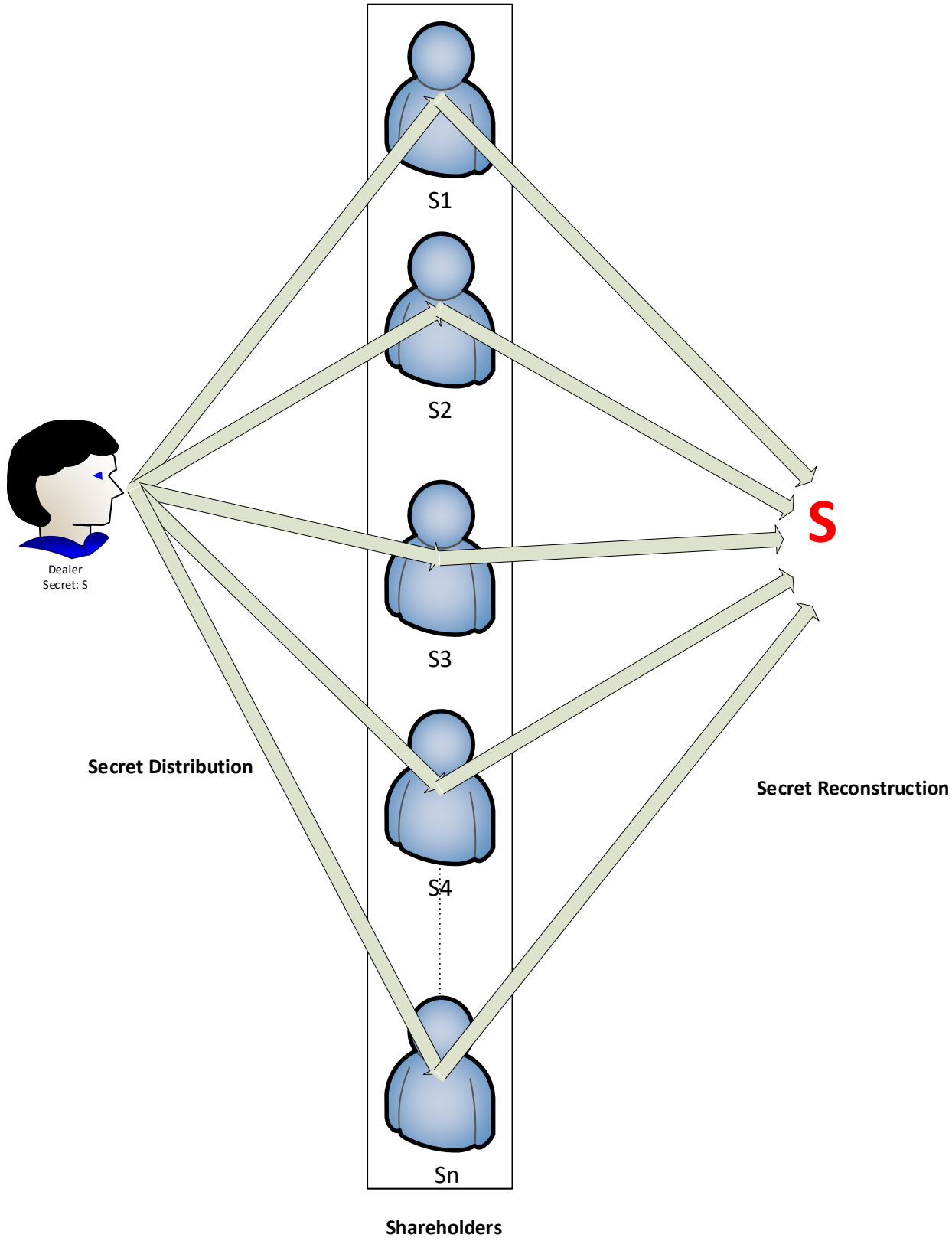

Fig. 3: Share distribution/reconstruction phase

4.1. Initialization process

In case dealer wants to select the n different non zero integers from over $\mathbb{Z}_p$, which indicates x_i, from $1 \leq i \leq n$. Here, these values can be accessed publicly.

4.2. Share distribution and reconstruction phases

1. Dealer D desires to share the secret information $k \in \mathbb{Z}_p$. Dealer D can choose the randomly $k-1$ integers for $\mathbb{Z}_p$ that can be signified as $c_1, c_2, c_3, \ldots c_{k-1}$; Additionally; $c_0 = K$.

2. Dealer D can compute $y_i = c(x_i)$, only for $1 \leq i \leq n$, hereunder

$c(x) = \sum_{j=0}^{k-1} c_j x^j \bmod p.$

3. Here, the dealer can give participants P_i their share y_i.

Briefly, dealer D can construct a random polynomial over degree $k-1$. However, the constant term for k secret information is $c_0 = k$. Each participant can obtain points over (x_i, y_i) regarding the polynomial equation. Furthermore, we can now verify two dissimilar properties, that is, Participants k in the group can construct anyone in the regard of polynomial $c(x)$and can calculate the secret; any group for $k-1$ participants cannot recover it.

Now, we will see how the k participants can recover the polynomial $c(x)$. Such action is fundamentally achieved in the sense of interpolation polynomial. Here, we assume that set $N = \{P_1, P_2, P_3, \ldots P_K\}$ from this set can reconstruct the secret. Participants in set *N* are:

$y_i = c(x_i), 1 \leq i \leq k,$

here, $c(x)$ belongs to $\mathbb{Z}_p[x]$. This secret information is chosen by the dealer D from the polynomial. Moreover, polynomial $c(x)$ has a degree $k-1$ that can be written as,

$c(x) = c_0 + c_1 x + c_2 x + \ldots . c_{k-1} x^{k-1}$

here, unknown coefficients $c_0, c_1, c_2, \ldots . c_k$ and $c_0 = k$ are secret information. Hence, every participant knows that $y_i = c(x_i)$ could achieve a system of the linear equation from the k unknowns $c_0, c_1, c_2, \ldots . c_{k-1}$. Group N contains k systems of a linear equation that are for discarding. Suppose that the equations are linearly independent. Hence, we will achieve a unique solution, and c_0 will be discovered as the reform of the key. The following is obtained under linear equation construction:

$c_0 + c_1 x_1 + c_2 {x_1}^2 + \ldots . c_{k-1} {x_1}^{k-1} = y_1,$
$c_0 + c_1 x_2 + c_2 {x_2}^2 + \ldots . c_{k-1} {x_2}^{k-1} = y_2,$
.
.
.
$c_0 + c_1 x_k + c_2 {x_k}^2 + \ldots . c_{k-1} {x_k}^{k-1} = y_k,$

This above equation can also be written in the form of the matrix,

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{K-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{K-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_K & x_K^2 & \cdots & x_K^{K-1} \end{pmatrix} \begin{pmatrix} c_o \\ c_1 \\ \vdots \\ c_K \end{pmatrix} = \begin{pmatrix} y_o \\ y_1 \\ \vdots \\ y_K \end{pmatrix}$$

The coefficient matrix is called A or a Vander-monde matrix. The well-known formula in the regard of a determinant of $k * k$ is called Vander-monde matrix.

$$\det A = \prod_{1 \leq i \leq j \leq k} (x_i - x_j) \bmod p$$

Suppose $p = 17, k = 3$, and $n = 5$. The range of public values x coordinates $x_i = i$, for each $1 \leq i \leq 5$. Suppose a set of $B = P_1, P_2, P_3$ and pools shares, that is, 8, 10, 11, exists, correspondingly. The polynomial for $c(x)$ is written as follows:

$c(x) = c_0 + c_1 x + c_2 x^2$

We can compute values in $c(1)$, $c(3)$, and $c(5)$ in the unidentified c_0,c_1, c_2 consequences would be in the three followings equations in z_{17}:

$c_0 + c_1 + c_2 = 8$
$c_0 + 3c_1 + 9c_2 = 10$
$c_0 + 5c_1 + 8c_2 = 11$

Solving the linear equation z_p provides us a polynomial equation $c(x) = 13 + 10x + 2x^2$. Therefore, the value of the secret is $k = c_0 = 13$.

Now, we can consider the second issue—what would be the effect if the group of $k-1$ members attempts to calculate secret information. As scheduled, we could end with the equation of $k-1$. Here, the equation k is unknown. We can only show secret information and the value of any secret information in z_p. Suppose secret k has y_0. Subsequently, the value of secret $k = c_0 = c(0)$, as we have already $y_0 = c(0)$. As we know,

$y0 = c(0)$

This equation will produce a kth system of a linear equation. The system of linear equation organized by the preceding $k-1$ system of the linear equation can show the result in k equations in between the k unknown values. Moreover, the coefficient matrix becomes a Vander-monde matrix, which is a distinctive solution, as mentioned previously.

Hence, each potential value $y0$ is the secret value of k. A distinctive polynomial $c_{y0}(x)$ like that,

$yi = c_{y0} = (xi).$

As for range$1 \leq i \leq k-1$, like that,

$y0 = c_{y0} = (0).$

In this regard, no value of any secret could follow the rule by the group of $k-1$ participants members. Moreover, they could not achieve information about secret values.

This method also provides us with an alternative way to construct the polynomial for $c(x)$, which is

grounded on the Lagrange interpolation formula in regard to polynomials equations. In simple words, we say this explicit formula is for the distinctive polynomial $c(x)$ degree, which most at $k-1$. This result happens when k have different points at $y_1 = c(x_1),\ y_2 = (x_3), \ldots y_k = c(x_k)$:

$$c(x) = \sum_{i-1}^{k} yi \prod_{i<j<k, j\neq i} \frac{x - x_j}{x_i - x_j}.$$

By substituting $x = x_i$, all terms will vanish without ith term, that is, yi.

Henceforth, any participant of k group could compute the $c(x)$by utilizing the interpolation formula. However, a particular group is interested in computing the $= c_0$, and we can simplify the group. However, in $k = c_0 = c(0)$ we substitute $x = 0$ with the Lagrange interpolation formula and obtain the following:

$$k = \sum_{i=1}^{k} yi \prod_{1\leq j\leq k, j\neq i} \frac{xj}{xj - xi},$$

here, an explicit formula ends each secret value.

4.3. Access structures and general SSS

In the previous section, we obtained (k, n) construction on the basis of the subset practiced to achieve secret information. According to further normal condition, we could indicate subsets that could qualify and achieve accurate secret information.

Suppose Γ count be a subset of $S, \Gamma \subseteq 2^q$. However, Γ subsets indicate that participants can calculate the secret information. After this scenario, Γ can call an access structure. Γ subsets are called authorized subsets. If $S \subseteq Q$, then we used to indicate Sset of different size shares against the participants/members in$S$. Here, we explain the following formal definition of general access sharing schemes.

Properties 1: In the regard of SSS against the access structure, Γ is a technique of distributing secret information k in between a set of n members in a proper way where secret information cannot be compromised. Here, our scheme holds two kinds of properties as follows:

1.If $S \in \Gamma$, then $H(K/S) = 0$
2. If $S \notin \Gamma$, then $H(B/S) \geq \log\alpha$,

here, we set a fixed value$\alpha > 1$.

Based on the definition, any eligible subset could achieve the secret information. However, any non-eligible subset S could be a bit uncertain about the secret information. However, the secret can be guessed by the accurate value with the probability at least $2^{-H(B/S)}$. We can see a (k, n) threshold scheme, and it has an access structure $\Gamma = \{S \subseteq Q; |S| \geq k\}$.

Definition 1: SSS in which $\alpha = |K|$ is called a perfect sharing scheme.

In a perfect sharing scheme, a non-eligible subset of members cannot achieve secret information. Moreover, an outsider could not achieve accurate information from group participants.

Definition 2: $|S| = |K|$ If the condition is perfect, then it is called an ideal SSS.

An ideal SSS contains the smallest size of every participant shared secret information. It is a very significant aspect when they distribute the secret, and it would be a small size of the share as needed. Furthermore, we reveal certain properties of Γ structure. Assume that's S is an eligible subset ($S \in \Gamma$), and we can add another member to the set of S. The output of the added set must then be eligible. In this way, an access structure must contain the following properties.

If $S \in \Gamma$ and $S \subseteq C \subseteq P$, then $C \in \Gamma$. This kind of structure is called a monotone access structure. As such, we can explain the closure of an access structure Γ, which is also written as

$cl(\Gamma)$=$\{C \subseteq P; S \subseteq C, S \in \Gamma\}$.

Readers could easily see that the access structure is monotone if $\Gamma = cl(\Gamma)$.

Let Γ be an access structure, and we want to construct a perfect SSS in the regard of monotone access structure $cl(\Gamma_0)$. The steps for initialization and share distribution are as follows:

4.3.1. Initialization phase

Suppose D-dealer wants to select any access structure Γ, which is $cl(\Gamma) = cl(\Gamma_0)$. Hence, we could write Γ as $\Gamma = \{S_1, S_2, S_3, \ldots . S_l\}$. Here, $S_i \subseteq P$ for $1 \leq i \leq l$, and $S_1, S_2, S_3, \ldots S_l$ is publicly secret information.

4.3.2. Share distribution phase

Suppose $K = \mathrm{Z}_m$. Hence, every $S_j = \{Q_{i1}, Q_{i2}, Q_{i3}, \ldots . Q_{ik}\}$ can easily do the following:

1. Dealer constructs a (k, k) threshold scheme in the regard of $k$aside of members S_j. Hence, a dealer can choose k in random values $c_{j1}, c_{j2}, c_{j3}, \ldots c_{jk}$ such that, $k = c_{j1} + c_{j2} + c_{j3}, \ldots . c_{jk} \bmod Z_m$
2. Dealer wants to publish values c_{jm} to member $Q_{im}, 1 \leq m \leq k$, in the small pieces as the members shared information

The small size of share for the member i is the set of pieces Q_i acknowledges. Here, the number of small pieces are similar to the number of times that is Q_i could be found in the$S_1, S_2, S_3, \ldots S_l$. We can construct an example to understand the above scenario.

Suppose,

$$\Gamma_0 = \{\{Q_1, Q_2, Q_4\}, \{Q_1, Q_3, Q_4\{Q_2, Q_3\}\} = \{S_1, S_2, S_3\}$$

and

$$k = Z_m.$$

Choose $\Gamma_0 = \Gamma$. In regard to every subset in Γ, we could design a (k, n)threshold scheme.

Starting with S_1, we can choose $c_1, c_2, c_3 \in z_m$ such as

$$K = c_1, c_2, c_3 \bmod Z_m,$$

here, we provide the piece c_1 to Q_1,c_2 to Q_2 as well $c_3$to Q_4. For S_2, we could choose $s_1, s_2, s_3 \in Z_m$ such that,

$$K = s_1, s_2, s_3 \bmod Z_m,$$

here we provide the piece $s_1$toQ_1, $s_2$to $Q_3$and s_3 toQ_4, after, for S_3we can choose $w_1, w_2 \in Z_m$ such that,

$$K = w_1 + w_2 \bmod Z_m.$$

We can give the piece w_1 to Q_2 and $w_2$to Q_3. The distribution of pieces would result in the following small shares: Q_1 has (c_1, s_1); Q_2 has (c_2, w_1); Q_3 has (s_2, w_2); and Q_4 has (s_3, w_3).

These results prove that construction gives the perfect sharing scheme. We neglect formal proof and only provide a draft. In any eligible subset S, $S_i \in \Gamma$ exists, such that $S_i \subseteq S$. In this scenario, members in S_i can pool their shares together and achieve the secret information K. In any non-eligible subset S, no $S_i \in \Gamma$ could exist. Suppose that $S_i \subseteq B$. Threshold schemes are very independent, which is enough to ruminate a scheme. However, subset S is not eligible in any of threshold schemes.S could not achieve information about the secret key in any threshold scheme.

The noticeable disadvantage of our construction is that the size of the share will be too large. In SSS, we need to give shares to the participants as small as possible during the distribution phase. If the share size is a bit large, then the adversary could attack shares and obtain secret data. Alternatively, the ideal SSS can be explored. However, this option is only viable for numerous access structures to demonstrate that they could not be comprehended by an ideal SSS.

5. Discussions

This section summarizes our proposed research work. The improvement against WSNs' security and SSS has been proposed consequently. We proposed a novel-based SSS. These schemes are very powerful during the implementation of any secure system. We performed substantial research on WSNs' security, especially in key transfer protocols. The majority of previous articles proposed different types of schemes in WSNs, but limited research has been proposed accordingly. We proposed SSS, access structure, and general SSS in a deep manner. Both schemes are very useful. Future researchers could implement these schemes in key transfer protocols in WSNs. These schemes give the new research directions in the field of sensor nodes and a key authentication between the groups of sensor nodes. Sensory data are very important during the deployment of the sensor's environment. Hence, the security of sensors nodes could be managed by using our proposed schemes.

6. Conclusion and future work

Security is the foremost apprehension for the energy-constrained WSNs under the comprehensive security application. In the current age, security is the focus of many works, and constructing powerful security protocols is very challenging. Many researchers proposed several authenticated schemes to achieve privacy and verify nodes. Most methods focused on the security of proposed schemes with the sensor's protocols application. In this article, we proposed a novel-based SSS, which can be used to transfer protocols within the WSN applications. Moreover, this scheme is theoretically secured. The proposed schemes give the new concepts of designed protocols, especially in the WSNs environment. Our scheme size of shares a bit large. However, we plan to decrease the size of the share in the upcoming enhancement.

Compliance with ethical standards

Conflict of interest

The authors declare that they have no conflict of interest.

References

Ali F, Khan MS, and Akhtar H (2019b). Security review in internet of things. Internet of Things and Cloud Computing, 7(3): 80-87. https://doi.org/10.11648/j.iotcc.20190703.14

Ali F, Yigang H, and Yi R (2019a). A novel security architecture of internet of things. International Journal of Computer Theory and Engineering, 11(5): 89-96. https://doi.org/10.7763/IJCTE.2019.V11.1249

Barker WC and Barker E (2008). Recommendation for the triple data encryption algorithm (TDEA) block cipher. NIST Special Publication (SP) 800-67 Revision 1. Available online at: https://bit.ly/2UTdr8t

Blakley GR (1979). Safeguarding cryptographic keys. In the AFIPS National Computer Conference, California, USA, 48: 313-317. https://doi.org/10.1109/MARK.1979.8817296

Blom R (1983). Non-public key distribution. In: Chaum D, Rivest RL, and Sherman AT (Eds.), Advances in cryptology: 231-236. Springer, Boston, USA. https://doi.org/10.1007/978-1-4757-0602-4_22

Blum M (1983). How to exchange (secret) keys. In the Fifteenth Annual ACM Symposium on Theory of Computing, Association for Computing Machinery, New York, USA: 440-447. https://doi.org/10.1145/800061.808775

Chan H, Perrig A, and Song D (2003). Random key predistribution schemes for sensor networks. https://doi.org/10.1184/R1/6469211.v1

Das ML (2009). Two-factor user authentication in wireless sensor networks. IEEE Transactions on Wireless Communications, 8(3): 1086-1090. https://doi.org/10.1109/TWC.2008.080128

Davis R (1978). The data encryption standard in perspective. IEEE Communications Society Magazine, 16(6): 5-9. https://doi.org/10.1109/MCOM.1978.1089771

Di Pietro R and Guarino S (2013). Data confidentiality and availability via secret sharing and node mobility in UWSN. In the INFOCOM, IEEE Computer and Communications Societies, IEEE Annual Joint Conference, IEEE, Turin, Italy: 205-209. https://doi.org/10.1109/INFCOM.2013.6566764

Eschenauer L and Gligor VD (2002). A key-management scheme for distributed sensor networks. In the 9th ACM Conference on Computer and Communications Security, ACM, Washington, USA: 41-47. https://doi.org/10.1145/586110.586117

Harn L and Lin C (2010). Authenticated group key transfer protocol based on secret sharing. IEEE Transactions on Computers, 59(6): 842-846. https://doi.org/10.1109/TC.2010.40

Harn L, Hsu CF, and Li B (2018). Centralized group key establishment protocol without a mutually trusted third party. Mobile Networks and Applications, 23(5): 1132-1140. https://doi.org/10.1007/s11036-016-0776-7

He D, Gao Y, Chan S, Chen C, and Bu J (2010). An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc and Sensor Wireless Networks, 10(4): 361-371.

He D, Kumar N, Chen J, Lee CC, Chilamkurti N, and Yeo SS (2015a). Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Systems, 21(1): 49-60. https://doi.org/10.1007/s00530-013-0346-9

He D, Kumar N, Wang H, Wang L, Choo KKR, and Vinel A (2016). A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network. IEEE Transactions on Dependable and Secure Computing, 15(4): 633-645.

He D, Zeadally S, and Wu L (2015b). Certificateless public auditing scheme for cloud-assisted wireless body area networks. IEEE Systems Journal, 12(1): 64-73. https://doi.org/10.1109/TDSC.2016.2596286

Hsu C, Zeng B, and Zhang M (2014a). A novel group key transfer for big data security. Applied Mathematics and Computation, 249: 436-443. https://doi.org/10.1016/j.amc.2014.10.051

Hsu C, Zeng B, Cui G, and Chen L (2014b). A new secure authenticated group key transfer protocol. Wireless Personal Communications, 74(2): 457-467. https://doi.org/10.1007/s11277-013-1298-2

Hsu CF, Harn L, He T, and Zhang M (2016). Efficient group key transfer protocol for WSNs. IEEE Sensors Journal, 16(11): 4515-4520. https://doi.org/10.1109/JSEN.2016.2538292

Jaiswal P and Tripathi S (2017). An authenticated group key transfer protocol using elliptic curve cryptography. Peer-to-Peer Networking and Applications, 10(4): 857-864. https://doi.org/10.1007/s12083-016-0434-7

Jiang Q, Chen Z, Li B, Shen J, Yang L, and Ma J (2018). Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. Journal of Ambient Intelligence and Humanized Computing, 9(4): 1061-1073. https://doi.org/10.1007/s12652-017-0516-2

Jiang Q, Ma J, Yang C, Ma X, Shen J, and Chaudhry SA (2017). Efficient end-to-end authentication protocol for wearable health monitoring systems. Computers and Electrical Engineering, 63: 182-195. https://doi.org/10.1016/j.compeleceng.2017.03.016

Khan E, Gabidulin E, Honary B, and Ahmed H (2012). Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks. IET Wireless Sensor Systems, 2(2): 108-114. https://doi.org/10.1049/iet-wss.2011.0097

Khan MK and Alghathbar K (2010). Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks.' Sensors, 10(3): 2450-2459. https://doi.org/10.3390/s100302450 **PMid:22294935 PMCid:PMC3264488**

Koga H and Honjo S (2014). A secret sharing scheme based on a systematic Reed-Solomon code and analysis of its security for a general class of sources. In the IEEE International Symposium on Information Theory, IEEE, Honolulu, USA: 1351-1355. https://doi.org/10.1109/ISIT.2014.6875053

Kurihara J, Kiyomoto S, Fukushima K, and Tanaka T (2008). A new (k, n)-threshold secret sharing scheme and its extension. In the International Conference on Information Security, Springer, Taipei, Taiwan: 455-470. https://doi.org/10.1007/978-3-540-85886-7_31

Laih CS, Lee JY, and Harn L (1989). A new threshold scheme and its application in designing the conference key distribution cryptosystem. Information Processing Letters, 32(3): 95-99. https://doi.org/10.1016/0020-0190(89)90008-2

Lee CY, Wang ZH, Harn L, and Chang CC (2011). Secure key transfer protocol based on secret sharing for group communications. IEICE Transactions on Information and Systems, 94(11): 2069-2076. https://doi.org/10.1587/transinf.E94.D.2069

Li F and Xiong P (2013). Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sensors Journal, 13(10): 3677-3684. https://doi.org/10.1109/JSEN.2013.2262271

Liu Y, Guo W, Fan CI, Chang L, and Cheng C (2018). A practical privacy-preserving data aggregation (3PDA) scheme for smart grid. IEEE Transactions on Industrial Informatics, 15(3): 1767-1774. https://doi.org/10.1109/TII.2018.2809672

Miller VS (1986). Use of elliptic curves in cryptography. In: Williams H C (Ed.), Advances in cryptology, Lecture Notes in Computer Science, 218, Springer, Berlin, Heidelberg, Germany. https://doi.org/10.1007/3-540-39799-X_31

NIST (2001). Announcing the advanced encryption standard (AES). National Institute of Standards and Technology, U.S. Department of Commerce, USA.

Omote K and Thao TP (2015). SW-SSS: Slepian-wolf coding-based secret sharing scheme. In the Computational Intelligence in Security for Information Systems Conference, Springer, Burgos, Spain: 347-365. https://doi.org/10.1007/978-3-319-19713-5_30

Pottie GJ and Kaiser WJ (2000). Wireless integrated network sensors. Communications of the ACM, 43(5): 51-58. https://doi.org/10.1145/332833.332838

Rasheed A and Mahapatra R (2011). Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks. IEEE Transactions on Parallel and Distributed Systems, 22(1): 176-184. https://doi.org/10.1109/TPDS.2010.57

Ruj S, Nayak A, and Stojmenovic I (2013). Pairwise and triple key distribution in wireless sensor networks with applications. IEEE Transactions on Computers, 62(11): 2224-2237. https://doi.org/10.1109/TC.2012.138

Sáez G (2003). Generation of key predistribution schemes using secret sharing schemes. Discrete Applied Mathematics, 128(1): 239-249. https://doi.org/10.1016/S0166-218X(02)00448-1

Schneier B (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). In: Anderson R (Ed.), Fast softwareencryption. Lecture Notes in Computer Science, 809, Springer, Berlin, Heidelberg, Germany. https://doi.org/10.1007/3-540-58108-1_24

Shamir A (1979). How to share a secret. Communications of the ACM, 22(11): 612-613. https://doi.org/10.1145/359168.359176

Shen J, Shen J, Chen X, Huang X, and Susilo W (2017b). An efficient public auditing protocol with novel dynamic structure for cloud data. IEEE Transactions on Information Forensics and Security, 12(10): 2402-2415. https://doi.org/10.1109/TIFS.2017.2705620

Shen J, Zhou T, He D, Zhang Y, Sun X, and Xiang Y (2017a). Block design-based key agreement for group data sharing in cloud computing. IEEE Transactions on Dependable and Secure Computing, 16(6): 996-1010. https://doi.org/10.1109/TDSC.2017.2725953

Sun DZ, Li JX, Feng ZY, Cao ZF, and Xu GQ (2013). On the security and improvement of a two-factor user authentication scheme in wireless sensor networks. Personal and Ubiquitous Computing, 17(5): 895-905. https://doi.org/10.1007/s00779-012-0540-3

Sun Y, Wen Q, Sun H, Li W, Jin Z, and Zhang H (2012). An authenticated group key transfer protocol based on secret sharing. Procedia Engineering, 29: 403-408. https://doi.org/10.1016/j.proeng.2011.12.731

Watro R, Kong D, Cuti SF, Gardiner C, Lynn C, and Kruus P (2004). TinyPK: Securing sensor networks with public key technology. In the 2nd ACM Workshop on Security of ad hoc and Sensor Networks, ACM, Washington, USA: 59-64. https://doi.org/10.1145/1029102.1029113

Wood AD and Stankovic JA (2002). Denial of service in sensor networks. Computer, 35(10): 54-62. https://doi.org/10.1109/MC.2002.1039518

Wu F, Xu L, Kumari S, and Li X (2017). A new and secure authentication scheme for wireless sensor networks with formal proof. Peer-to-Peer Networking and Applications, 10(1): 16-30. https://doi.org/10.1007/s12083-015-0404-5

Xue K, Ma C, Hong P, and Ding R (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network and Computer Applications, 36(1): 316-323. https://doi.org/10.1016/j.jnca.2012.05.010

Yeh HL, Chen TH, Liu PC, Kim TH, and Wei HW (2011). A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors, 11(5): 4767-4779. https://doi.org/10.3390/s110504767 **PMid:22163874 PMCid:PMC3231356**

Yuan W, Hu L, Li H, and Chu J (2013). Security and improvement of an authenticated group key transfer protocol based on secret sharing. Applied Mathematics and Information Sciences, 7(5): 1943-1949. https://doi.org/10.12785/amis/070532

Zhang K, Xu K, and Wei F (2018). A provably secure anonymous authenticated key exchange protocol based on ECC for wireless sensor networks. Wireless Communications and Mobile Computing, 2018: 2484268. https://doi.org/10.1155/2018/2484268