Secret Sharing Based Key Agreement Protocol for Body Area Networks

Weihong Sheng[1], Bin Cai[1(✉)], Chunqiang Hu[1], and Ruinian Li[2]

[1] School of Big Data and Software Engineering, Chongqing University, China
im.swh@outlook.com, {caibin,chu}@cqu.edu.cn
[2] Computer Science Department, Bowling Green State University, USA
lir@bgsu.edu

Abstract. In order to provide more comprehensive medical services and personalized health monitoring according to individual needs, Body Area Networks (BANs) have been extensively studied by many researchers. As BANs involve the transmission of personal private data, the security of the communication is of utmost importance. Unfortunately, existing encryption techniques cannot be directly applied with the limited power or computation ability of the sensors in BANs. An alternative direction is to use physiological signals for key agreement. However, many of the current physiological signal-based key agreement schemes either have high overheads or are vulnerable to certain security issues. In this paper, we proposed a novel secret sharing and Bloom filter based key agreement scheme that balances overhead and security for BANs. Also, we use an approximate hash table to free ourselves from the problem of dependence on the ordering of features, which has been neglected by previous researchers. We validate the security of our scheme with based on real datasets and compare overheads with other solutions.

Keywords: Body Area Networks · Key Agreement · Physiological Signals · Secret Sharing.

1 Introduction

E-health entails the comprehensive application of communication technology in healthcare, spanning disease prevention, diagnosis, treatment, and recovery. It addresses issues of non-openness and transparency in medical information, while also to some extent integrating scattered medical resources. With the rapid advancement of embedded technology, an increasing number of sensors are being integrated into wearable devices, also known as smart sensors, enabling them to offer personalized and customized healthcare services.

Various types of devices communicate within the human body domain via wireless networks, forming Body Area Networks (BANs). BANs essentially represent a specialized form of the Internet of Things (IoT), differing in their use of sensor nodes with lower performance and shorter battery life. In BANs, it is essential to facilitate end-to-end transmission of collected data between sensors.

This data may contain identifiable biological information about the user, which is inherently private and highly sensitive. Therefore, ensuring a higher level of security in the communication process is imperative compared to traditional IoT systems [10, 13, 16, 17].

To meet security and privacy requirements, data-encrypted transmission is widely used for data security protection today [8, 9]. Encryption ensures the confidentiality and integrity of the data. If data are transmitted in plain text, users cannot avoid the risk of eavesdropping, replay attacks, or even tampering by attackers [2, 12]. Because biological data concern the physiological health of the user, tampering can lead to serious consequences such as misdiagnosis, posing significant risks to the user's life and property safety.

Modern encryption techniques encompass both symmetric and asymmetric encryption. One notable drawback of asymmetric encryption systems is their increased demand for system resources in computation or storage. Sensors within BANs are constrained by various application scenarios, such as being implanted in the human body or worn on the body. These limitations make it challenging for them to accommodate significant overheads in computation, storage, and battery usage. For instance, in the case of implanted sensors, also known as Implantable Medical Devices (IMDs), surgical procedures are often necessary for battery replacement once they are depleted. Consequently, the frequent adoption of elliptic curve-based asymmetric encryption systems is restricted by the limited resources available for such sensors.

Originally researchers used the form of pre-deployed secret messages to study how to design key agreement protocols. This approach was abandoned due to its lack of scalability and the potential security risks it posed. Sensors collect a variety of physiological signals that are unique and distinguishable in the human body, such as heartbeat and blood pressure. This data, which can be observed in almost all areas of the human body, are valuable assets that can be utilized for key agreement and have been extensively researched by scholars. Hence, researchers prefer symmetric encryption systems that require less computation overhead. Thus, the key to achieving security is to create a secure protocol for the confidential exchange of keys.

Previous studies [6, 15] have assumed the feasibility of obtaining accurate feature sequences from physiological signals that exhibit strong ordering. For instance, let f_1, f_2, f_3, f_4, f_5 and $f'_1, f'_2, f'_3, f'_4, f'_5$ represent feature sequences generated by two sensors located at different parts of the same body. In an ideal scenario, $f_i = f'_i$ for $i \in 1, 2, 3, 5$, indicating that some features differ while others remain the same. Consequently, the two sensors can share a common secret, enabling the establishment of a secure communication channel based on shared equal features. However, false positives during physiological signal detection can lead to the insertion of additional peaks into feature sequences, causing misalignment between f_i and f'_i. For example, the actual situation may involve $f_1 = f'_1, f_3 = f'_2, f_4 = f'_3, f_5 = f'_4$. However, from the sensors' perspective, misalignment results in $f_1 = f'_1, f_2 \neq f'_2, f_3 \neq f'_3, f_4 \neq f'_4, f_5 \neq f'_5$ if the misalignment issue is disregarded. The problem of misalignment, which significantly

affects the success rate of feature matching, has been overlooked by previous researchers.

In this paper, we propose a Secret Sharing Based Key Agreement scheme (SSKA). SSKA employs the Shamir secret sharing scheme to maintain the encryption key as a confidential matter, enabling the parties to securely exchange keys. The main contribution as follows:

- We present a new key agreement protocol that strikes a balance between security and overhead by combining Shamir's secret sharing and Bloom filter.
- We tackle the problem of misalignment by utilizing an approximate hash table, which requires a bit more communication and computation.
- We conduct complete simulations utilizing genuine datasets.

2 Related Work

2.1 Quantification of Physiological Signals

Xu et al. [14] demonstrated that the last 4 bits under the binary representation of Inter-Pluse-Interval (IPI) have almost complete randomness. Venkatasubramanian et al. [11] proposed a method to quantify physiological signals by using an augmented fast Fourier transform to generate features. Chizari et al. [4] analyzed the physiological signals with respect to important features such as ubiquity, activity, robustness, persistence, and uniqueness, and noted that the last 3 features have not yet been systematically examined in the current methods for randomness extraction from IPI. The study proposed methods to measure the latter 3 features and concluded that extraction of strongly uniform random numbers from IPI is not possible. The authors suggested using the trend of the IPI rather than its specific values and proposed a new method for randomness extraction.

2.2 Key Agreement Methods

It has been suggested by some researchers that human physiological signals can be used to create secure communication between each sensor device in BANs, without taking into account the premise of secure communication between BANs and remote third parties. Examples of such biometrically independent physiological signals are Electrocardiography (ECG or EKG) and Photoplethysmogram (PPG), which can be detected in different parts of the body with similar characteristics. Cherukuri et al. [3] proposed that these signals can be used to generate inter-sensor sharing session keys. Venkatasubramanian et al. [11] observed that the Hamming distances of IPI obtained from the same human body and from different human bodies are 60 and 65, respectively. This is due to the fact that IPI is encoded as binary, and translational and rotational errors can lead to very different values.

In order to take advantage of the fact that similar yet distinct physiological signals can be obtained from different parts of the human body, many researchers have proposed their own solutions based on fuzzy vaults. Hu et al. [6] proposed

Ordered-Physiological-Feature-based Key Agreement (OPFKA) which has lower computational consumption and higher security compared to PSKA. Zheng et al. [18] analyzed fuzzy vault and fuzzy commitment in the context of ECG-based key agreement, and concluded that fuzzy commitment-based schemes have better false acceptance rates, while fuzzy vault-based schemes can achieve lower false positives with lower overhead. Hodgkiss et al. [5] proposed a rotation-assisted fuzzy vault scheme to enhance the security of using fuzzy vault construction.

3 Background

3.1 Physiological Signals

ECG is a signal that records the electrophysiologic activity of the heart in units of time. The signal travels from the heart through various organs and tissues of the body and can eventually be detected on the body surface. Although the heartbeat activity of the human body is regular, the electrical currents generated at the microscopic level do not exactly conform to this pattern. Because the human heart rate is controlled by its parasympathetic nerves and can be affected by factors brought about by biological rhythms, human activity, respiration, and temperature, it has a certain degree of randomness and unpredictability and can be used as a source of random number generation.

3.2 Shamir's Secret Sharing

Shamir's secret sharing scheme is based on polynomial interpolation over a finite field. Suppose we have a secret S, which we share with n participants, each of whom holds a piece of S, denoted as $S_1, S_2, ..., S_n$. We agree on a threshold value t in advance before splitting the secret, and the secret can be recovered if and only if the number of participants involved in the recovery of the secret is $\geq t$.

The basic idea of the scheme is based on the Lagrange interpolation theorem. Let us assume that the secret S comes from a finite field and we choose $t-1$ random numbers $a_1, a_2, ..., a_{t-1}$ from the same finite field. Construct the polynomial:

$$f(x) = S + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \tag{1}$$

Then, for positive integers $i \leq n$, let us assume $S_i = (i, f(i))$ and share S_i to participant i. To recover the secret, it is sufficient for any t participants to cooperate and recover the secret by the following formula:

$$f(0) = \sum_{j=0}^{t-1} y_j \prod_{\substack{m=0 \\ m \neq j}}^{t-1} \frac{x_m}{x_m - x_j} \tag{2}$$

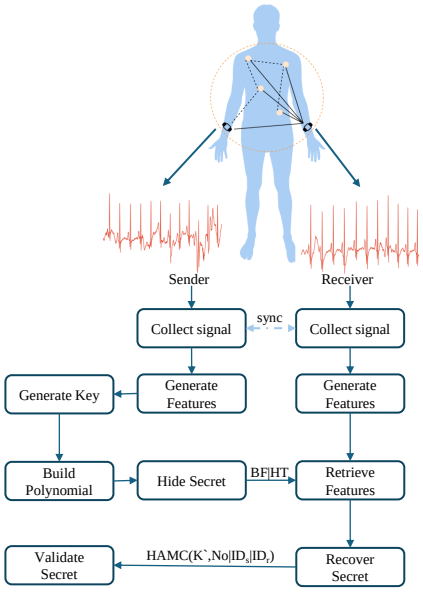

Fig. 1. The Process of SSKA

4 Our Scheme

In this section, we introduce our Secret Sharing based Key Agreement scheme. Our scheme utilizes the fact that physiological signals from different parts of the same human body are similar, but not identical. That is, the ideal IPI signals captured in different parts of the same human body should be mostly the same with small differences. We aim to maximize the use of this similarity to securely implement key exchange. The whole scheme process is shown in Fig. 1, which consists of three processes: feature generation, secret sharing, and secret recovery. We assume that the key agreement occurs between two sensors s and r in different parts of the human body. s and r are the sender and receiver of the key agreement process, respectively.

4.1 Feature Generation

Alg. 1 describes the phrase of feature generation. In this phase, we use the XQRS algorithm to obtain the QRS peak cluster locations, and then use the correction algorithm to correct whole QRS peak cluster indexes. The IPI sequence is obtained by calculating the difference between the neighboring R-peak indices.

Since using IPI sequence directly may leak privacy, we need to extract features with enough randomness. Xu et al. [14] showed that the last 4 bits of the IPI have a high degree of randomization, and several studies also utilized this property for key agreement. Thus, this technique is also adopted by SSKA. For

simplicity, we reuse IPI to refer to the last 4 bits of IPI. To avoid false positives during secret sharing and reduce overhead in feature generation, we design a sliding window to extract features with length $k/4$ and step p where k is the length of features. For example, f_s^1 is extracted from $\{IPI_1, .., IPI_{k/4}\}$ and f_s^2 is extracted from $\{IPI_{1+p}, ..., IPI_{k/4+p}\}$.

Algorithm 1 The Process of Feature Generation

Input: raw data, window length $k/4$, step size p, feature length k, feature number N
Output: F_s

```
xqrs ← XQRS(raw data). //obtaining QRS peak group indexes using the XQRS algorithm
{R_i} ← search local maximum of xrqs. //Searching for local maxima in QRS to obtain R-peak indexes
for Iterate over {R_i} do
    IPI_i ← R_{i+1} − R_i
end for
for Iterate over IPI with l do
    {c_0, c_1, c_2, ..., c_{k/4}} ← extract last 4 binary of IPI_i, IPI_{i+1}, IPI_{i+2}, ..., IPI_{i+k/4}
    f_s^j ← c_0 ⊕ c_1 ⊕ c_2 ⊕ ... ⊕ c_{k/4}
    if j ≤ N then
        stop
    end if
end for
F_s = {f_s^1, f_s^2, ..., f_s^N}
return F_s
```

Similarly, the receiver r eventually produces $F_r = \{f_r^1, f_r^2, ..., f_r^N\}$.

4.2 Secret Sharing

Alg. 2 is the secret sharing process. With features F_s, s can build the polynomial by choosing the first $t-1$ features as the constants of the polynomial and K, which is a random key generated by s, as the secret S to be shared:

$$f(x) = K + f_s^1 x + f_s^2 x^2 + \cdots + f_s^{t-1} x^{t-1} \tag{3}$$

After completing the building of the polynomial, N secret pieces $\left(f_s^i, f\left(f_s^i\right)\right)$ are generated by using all the feature values as inputs x.

We use a Bloom filter BF to hide the secret pieces to be shared. m is the length of BF and q is the number of hash functions that affect the false positive rate (FPR) and computational overhead. We will discuss the parameter setting in experiments.

To handle the misalignment problem, we introduce an approximate hash table HT. Each polynomial value $f\left(f_s^i\right)$ is placed in the corresponding position $addr \leftarrow SHA(f_s^i)\%\alpha$. If a collision occurs, the polynomial value is inserted at the end of the chain table at the corresponding position.

After the above processes, s sends a message $HT|BF$ to r without encryption.

Algorithm 2 The Process of Secret Sharing

Input: secret K, HT size α, threshold t, feature sequence F_s, hash family $H = \{h_1, ..., h_q\}$
Output: HT, BF,

```
HT ← 2d linked list with length α
BF ← 1d array with length m
for iterate over F_s do
    calculate f(f_s^i)
    addr ← SHA(f_s^i)%α
    add f(f_s^i) to HT[addr]
    for h ∈ H do
        BF[h(f_s^i)] = 1
    end for
end for
return HT, BF
```

Algorithm 3 The Process of Secret Recovery

Input: hash table HT, Bloom filter BF, feature sequence F_r, threshold t
Output: K'

```
j = 0
for iterate over F_r do
    if f_r^i ∈ BF then
        j ← j + 1
        calculate f(f_r^i)
        addr ← SHA(f_r^i)%α
        remove f(f_r^i) from HT[addr]
        if j ≤ t then
            stop
        end if
    end if
end for
K' ← using Lagrange interpolation
return K'
```

4.3 Secret Recovery

After the sensor r receives the message, it needs to retrieve the matched features mapped into BF. At this point, r has generated its own sequence of features F_r. According to the predefined hash family H, r matches the features mapped to BF one by one until it finds the set of features that satisfies the threshold value t. Once the matched features are found, the corresponding polynomial values

in HT are retrieved. Finally, the polynomial is reconstructed using Lagrange interpolation to solve the hidden secret K'.

The process of verifying that the encryption key has been successfully established is relatively simple, the sensor r simply uses its own recovered key K', to generate the HMAC $HMAC(K', N_o|ID_s|ID_r)$ where N_o is a timestamp, ID_s and ID_r are the ID of s and r, respectively. If s can decode the message using its own key K, then the key agreement is successful.

5 Security Analysis

5.1 Experiment Setting

The dataset used in this paper is from physinoet.org, contributed by Vollmer et al. [1]. The dataset consists of 13 participants, each wearing five types of sensors at the same time to collect physiological signals in a synchronized manner.

We choose ECG data collected by the clinically certified SOMNOtouch NIBP sensor as the experimental data. The sampling frequency of this data is 256Hz, and 4 copies of synchronized physiological data from different locations (ECG0, ECG1, ECG2, ECG3) will be collected for each participant. We divide them into two groups, one for ECG0 and ECG1 which are closer to the heart, and one for ECG2 and ECG3 which are slightly away from the heart.

We selected the first $40,000$ sample points of each participant's ECG, and then divided the $40,000$ sample points into 10 portions of the $4,000$ sample points each in order to generate 30 features.

With the suggestion of [15] that makes FPR $\leq 1^{-1024}$, if we set $N = 30$, we should take $p = 4, q = 10, m = 433, k = 64$.

5.2 Distinguishability

Distinguishability refers to the ability of key agreement protocols deployed in BANs to recognize and distinguish physiological signals of the same human body or different human bodies. In general, key agreement protocols make full use of the distinguishability of human physiological signals to achieve their own distinguishability. We use false reject rate (FRR) to evaluate the failure rate of key agreement on the same human body.

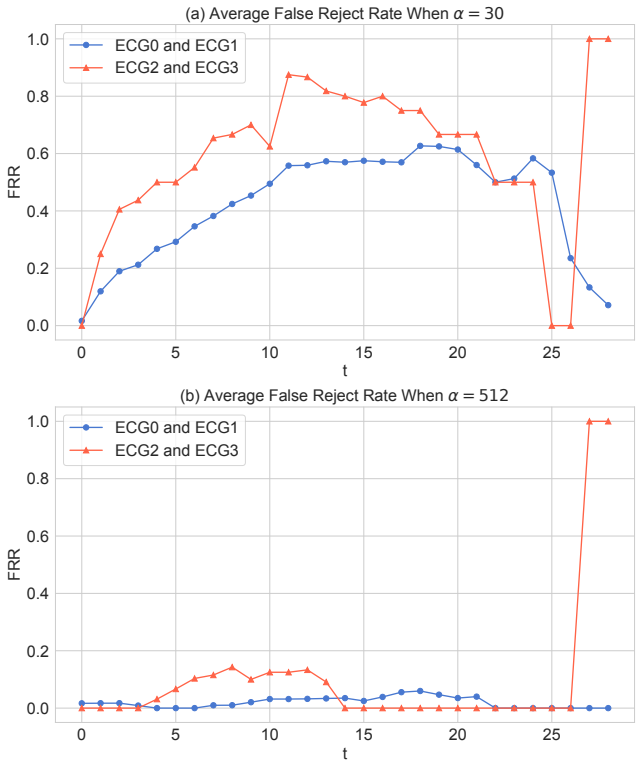

Fig. 2. Average False Reject Rate When $\alpha = 30$ or $\alpha = 512$

Fig. 2(a) shows the average false reject rate when the size of HT $\alpha = 30$. ECG0 and ECG1 have lower FRR than ECG2 and ECG3 because they are closer to the heart than the latter. ECG2 and ECG3, on the other hand, because they are far from the heart, have a very high FRR after threshold $t \leq 26$. The overall FRR in Fig. 2(a) is relatively high. The reason for this is that the size of the HT is too small, constrained by α, resulting in a high number of collisions. In order to reduce the collisions, it is worthwhile to make $\alpha = 512$, and Fig. 2(b) shows the average false reject rate after modifying the size of the HT. It can be seen that in the range of $t \leq 26$, the FRRs are less than 0.13, and the FRR of ECG0 and ECG1 is even almost 0. Therefore, to keep the FRR low, the size of the HT should be large enough. It should be noted that even with $\alpha = 512$, the actual space overhead of HT remains the same as when $\alpha = 30$.

6 Performance Analysis

The overall overhead is shown in Table. 1 with some similar works. Due to variances in implementation methodologies among distinct schemes, we conduct a

comparative analysis of overhead differences by scrutinizing the generic computational operations employed.

Table 1. Compare of Overhead [15]

Scheme	Storage	Communication	Computation	Security
BDK [19]	12500	$5252 \sim 25228$	4970	128
PSKA [11]	22500	22612	4970	121
OPFKA [6]	1220	$12632 \sim 12656$	4970	122
SGenP [7]	1220	1368	30	128
BFG [15]	72	$172 \sim 185$	300	131
SSKA	534	566	330	128

6.1 Storage Overhead

Since the overheads of identifiers, physiological features, hash values, message authentication codes, and key storage are similar in different schemes, we only needs to consider the overhead of storing feature vectors or vaults for the convenience of comparison. Table. 1 lists the minimum storage overhead of some schemes. In SSKA, the sensor mainly needs to store BF and HT, and the total storage overhead is $433 + 128 \times 30 = 4273$ bits, about 534 bytes. It is not as good as BFG but is better compared to the rest of the schemes. Here the reason for the size of each element in HT to be 128 bits is that while computing the polynomial we use the 12th Mersenne prime number $2^{127} - 1$. So for the sake of estimation, it is estimated here to be 128 bits.

6.2 Communication Overhead

In SSKA, there are only three communications. Since the first communication only consists of a synchronization signal sent by the initiator of the communication, its overhead can be neglected and the main communication overhead is generated by the last two communications. For the second communication, the sender sends the BF and HT, and for the third communication the receiver sends the hash message authentication code. The overhead of the BF and HT is about 534 bytes, and the overhead of the hash message authentication code is 256 bits. The total communication overhead is 566 bytes.

6.3 Computation Overhead

Currently, almost all physiological signaling-based key agreement schemes are based on hashing, message authentication codes, and arithmetic operations, and their computation overheads do not differ much. For comparison, we use the number of hashes to evaluate the computation overhead of SSKA. Similar to BFG, SSKA also performs 300 hashes and an additional 30 hash operations are used to hide polynomial values. Therefore, the hashing overhead of SSKA is 330.

6.4 Security Strength

In the above analysis, SSKA is worse than BFG in terms of storage, communication and computation overheads. Even in measuring the security strength, the security strength of BFG is higher than SSKA. However, the 131 bits security strength of BFG refers to the security of the key agreement phase, whereas the security strength of SSKA is the length of the generated key, which is 128 bits. This is because the key of BFG is simply generated from the same features through a hash function, and its individual features have a value space of 12 bits. Although its key length depends on the hash function used, it is vulnerable to attacks from historical physiological data leakage due to the direct use of features. SSKA, on the other hand, has a security level of $C_{2^{64}}^{t}$ in the key agreement phase, which is much more than 131 bits. Thus, although the overhead of SSKA is larger than BFG, the security strength is much stronger than BFG.

7 Conclusion

In this paper, we propose a Secret Sharing based Key Agreement Protocol, SSKA. This scheme satisfies the high security strength key Agreement process within acceptable performance overhead. With the combination of secret sharing, Bloom filter and approximate hash table, the protocol not only solves misalignment problem, but also has the features of plug and play, key scalability, high security strength and low overhead. The results of our simulation experiments show that our scheme has high security in the secret sharing process. And the lower FRR proves the practicality of our scheme.

Acknowledgments. This research was supported partially by Science and Technology Innovation Key R&D Program of Chongqing (CSTB2023TIAD-STX0036), Sichuan Science and Technology Program (No.2023YFQ0029, 2023YFQ0028), and National Natural Science Foundation of China (Nos.62372075, 62072065).

References

1. Bläsing, D., Buder, A., Reiser, J.E., Nisser, M., Derlien, S., Vollmer, M.: Ecg performance in simultaneous recordings of five wearable devices using a new morphological noise-to-signal index and smith-waterman-based rr interval comparisons. PLOS ONE **17**(10), 1–21 (10 2022)
2. Chen, S., Yu, D., Zou, Y., Yu, J., Cheng, X.: Decentralized wireless federated learning with differential privacy. IEEE Transactions on Industrial Informatics **18**(9), 6273–6282 (2022)
3. Cherukuri, S., Venkatasubramanian, K.K., Gupta, S.K.: Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In: Proc. Int. Conf. Parallel Process. Workshops. pp. 432–439. IEEE (2003)
4. Chizari, H., Lupu, E.: Extracting randomness from the trend of ipi for cryptographic operations in implantable medical devices. IEEE Trans. Dependable Secure Comput. **18**(2), 875–888 (2019)

5. Hodgkiss, J., Djahel, S.: Securing fuzzy vault enabled authentication in body area networks-based smart healthcare. IEEE Consum. Electron. Mag. **11**(1), 6–16 (2020)
6. Hu, C., Cheng, X., Zhang, F., Wu, D., Liao, X., Chen, D.: Opfka: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. In: Proc IEEE INFOCOM. pp. 2274–2282. IEEE (2013)
7. Kumari, P., Anjali, T.: Symmetric-key generation protocol (sgenp) for body sensor network. In: IEEE Int. Conf. Commun. Workshops, ICC Workshops - Proc. pp. 1–6. IEEE (2018)
8. Liu, Z., Hu, C., Li, R., Xiang, T., Li, X., Yu, J., Xia, H.: A privacy-preserving outsourcing computing scheme based on secure trusted environment. IEEE Transactions on Cloud Computing **11**(3), 2325–2336 (2023). https://doi.org/10.1109/TCC.2022.3201401
9. Liu, Z., Hu, C., Ruan, C., Hu, P., Han, M., Yu, J.: An enhanced authentication and key agreement protocol for smart grid communication. IEEE Internet of Things Journal pp. 1–1 (2024). https://doi.org/10.1109/JIOT.2024.3381379
10. Liu, Z., Hu, C., Ruan, C., Li, R.: A novel certificateless authentication and key agreement protocol for smart grid. In: GLOBECOM 2023 - 2023 IEEE Global Communications Conference. pp. 3288–3293 (2023). https://doi.org/10.1109/GLOBECOM54140.2023.10437238
11. Venkatasubramanian, K.K., Banerjee, A., Gupta, S.K.S.: Pska: Usable and secure key agreement scheme for body area networks. IEEE Trans Inf Technol Biomed **14**(1), 60–68 (2009)
12. Xiong, Z., Cai, Z., Hu, C., Takabi, D., Li, W.: Towards neural network-based communication system: attack and defense. IEEE Transactions on Dependable and Secure Computing (2022)
13. Xiong, Z., Li, W., Cai, Z.: Federated generative model on multi-source heterogeneous data in iot. In: Proceedings of the AAAI Conference on Artificial Intelligence. vol. 37, pp. 10537–10545 (2023)
14. Xu, F., Qin, Z., Tan, C.C., Wang, B., Li, Q.: Imdguard: Securing implantable medical devices with the external wearable guardian. In: Proc IEEE INFOCOM. pp. 1862–1870. IEEE (2011)
15. Yao, X., Liao, W., Du, X., Cheng, X., Guizani, M.: Using bloom filter to generate a physiological signal-based key for wireless body area networks. IEEE Internet Things J. **6**(6), 10396–10407 (2019)
16. Zhang, H., Zou, Y., Yin, H., Yu, D., Cheng, X.: Ccm-fl: Covert communication mechanisms for federated learning in crowd sensing iot. Digital Communications and Networks (2023)
17. Zhang, H., Zou, Y., Yu, D., Yu, J., Cheng, X.: Covert communications with friendly jamming in internet of vehicles. Vehicular Communications **35**, 100472 (2022)
18. Zheng, G., Shankaran, R., Yang, W., Valli, C., Qiao, L., Orgun, M.A., Mukhopadhyay, S.C.: A critical analysis of ecg-based key distribution for securing wearable and implantable medical devices. IEEE Sensors J. **19**(3), 1186–1198 (2018)
19. Zhou, J., Cao, Z., Dong, X.: Bdk: secure and efficient biometric based deterministic key agreement in wireless body area networks. In: Proc. Int. Conf. Body Area Networks - BODYNETS. pp. 488–494 (2013)