Hindawi
Security and Communication Networks
Volume 2021, Article ID 8527068, 8 pages
https://doi.org/10.1155/2021/8527068

Research Article

IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security

ChunHua Cao,[1,2] YaNa Tang,[1] DeYan Huang,[1] WeiMin Gan,[1] and Chunjiong Zhang[3]

[1]*Software Engineering Institute of Guangzhou, Guangzhou 510990, China*
[2]*University of Perpetual Help System, Manila 0900, Philippines*
[3]*Department of Computer Science, Tongji University, Shanghai 201804, China*

Correspondence should be addressed to Chunjiong Zhang; chunjiongzhang@tongji.edu.cn

Received 24 August 2021; Accepted 7 September 2021; Published 20 September 2021

Academic Editor: Jian Su

Wireless sensor networks (WSN) have problems such as limited power, weak computing power, poor communication ability, and vulnerability to attack. However, the existing encryption methods cannot effectively solve the above problems when applied to WSN. To this end, according to WSN's characteristics and based on the identity-based encryption idea, an improved identity-based encryption algorithm (IIBE) is proposed, which can effectively simplify the key generation process, reduce the network traffic, and improve the network security. The design idea of this algorithm lies between the traditional public key encryption and identity-based public tweezers' encryption. Compared with the traditional public key encryption, the algorithm does not need a public key certificate and avoids the management of the certificate. Compared with identity-based public key encryption, the algorithm addresses the key escrow and key revocation problems. The results of the actual network distribution experiments demonstrate that IIBE has low energy consumption and high security, which are suitable for application in WSN with high requirements on security.

1. Introduction

WSN is a wireless network composed of sensor nodes in the form of self-organization, which collects and processes the relevant information of monitored objects in the target area and sends it to the observer [1–10].

As early as the middle of the last century, there appeared a network which combined sensors with wireless transmitters and carried out real-time data acquisition, which was the prototype of WSN. WSN began to mature, following the technical progress and the deepening of related research [11–14]. The application field of WSN has gradually developed from the military field to all walks of life, such as agricultural production, environmental monitoring, cultural relics protection, and medical care [15]. Information encryption is the most core and basic technical method to protect information security [16–18]. The encryption process of data is to use encryption key and encryption algorithm to convert plaintext into ciphertext form that other users cannot understand, while decryption is the reverse process, using decryption key and decryption algorithm to recover the ciphertext into plaintext. Encrypted text is transmitted between users, and only the user with the decryption key can decrypt the encrypted text to obtain the plaintext [19–21]. In general, cryptosystems are divided into two types: one is symmetric cryptosystems and the other is public key cryptosystems.

Since WSN is usually deployed in an unattended environment, besides eavesdropping attacks, denial of service attacks, and other attacks faced by ordinary networks, it also faces the problems that WSN nodes are easy to be captured and counterfeited, and transmitted data are easy to be eavesdropped and tampered [22–24]. Currently, WSN has mediocre solution when facing the above security problems. Before these problems are solved, users cannot easily accept and deploy a WSN with security and data protection, which greatly limits WSN practical application.

In order to address the challenge of WSN security, IIBE is proposed. The main contributions of this paper are as follows:

(1) Compared with the traditional public key encryption, this algorithm does not need a public key certificate and avoids the management of certificates

(2) Compared with other existing identity-based encryption algorithms, this algorithm solves the problem of key escrow and key revocation

The rest of the paper is organized as follows. In Section 2, a literature review is studied in detail, while Section 3 provides the detailed methodology. Section 4 provides detailed results and discussion. Finally, the paper is concluded in Section 5.

2. Literature Review

At present, scholars have studied the improvement of symmetric/asymmetric encryption algorithms, the combination of various encryption algorithms, and some innovative encryption ideas.

Mostafaei et al. [22] provided a solution to the flooding attack in WSN through message digest algorithm combined with public key encryption, which improved the network's ability to detect data packet transmission. NS2 simulation results show that this method is effective in preventing flooding attacks. However, this method only signs the data transmitted by nodes to prevent flooding attacks and has limited preventive effect on data eavesdropping attacks, so it needs to be combined with other encryption methods in practical applications.

Rachkidy et al. [23] proposed a method of data storage combined with homomorphic encryption for some wireless sensor networks with insensitive real-time data, which is called DIOS. In some WSN (such as underwater sensor networks), people are more concerned about the whole data, rather than the data at a certain time. In view of this situation and considering that a large amount of data may cause loss to the sensor nodes if it is transmitted for a long time and a long distance, this literature puts forward that the data should be stored in a relay node in advance and preprocessed, so as to avoid the scattered and uninterrupted transmission of data. At the same time, homomorphic encryption is adopted to ensure security. This method is effective in some occasions, saving energy, and data can be stored safely. However, it is not suitable for most net-laying environments and has certain limitations.

Daniela and Giovanni [24] improved the application of AES in WSN, put forward the encryption idea of seven rounds of encryption, and combined with the table lookup method to optimize each round of operation. The results of simulation test show that the algorithm has greatly improved operation efficiency, and the speed is 13 times higher than that of common AES algorithm with less than 1 KB storage space. Although the security is lower than the traditional AES encryption algorithm, it is still suitable for WSN with limited energy.

All the above methods have defects, which cannot fully meet the needs of practical application of wireless sensor networks. To solve the above problems, according to the characteristics of WSN and based on the idea of identity-based encryption, an improved identity-based encryption algorithm (IIBE) is proposed, which can effectively simplify the key generation process, reduce the network traffic, and improve the network security.

3. Methodology

3.1. Analysis of WSN Network Topology and Its Security Problems. According to ZigBee protocol, WSN has three topologies: star topology, tree topology, and mesh topology, as shown in Figure 1.

The network specified by ZIGBEE protocol is composed of main coordinator nodes, router nodes, and terminal nodes, and there is only one main coordinator network. Every device in the network, including master device and slave device, has a unique 64-bit long address (IEEE address) built in at the factory. After the network is built, each slave device will be randomly assigned to a unique 16-bit short address code in the network by the master coordinator. The long address code is an absolute address, while the short address code is a relative address. Based on a large amount of data and practical operation experience of wireless sensor networks, it can be concluded that the existing wireless sensor networks have problems such as limited energy, limited computing and storage capacity, periodicity of data collection, asymmetry of data flow, and limited communication channel width.

Taking the WSN network designed by ZIGBEE protocol as an example, the more serious attack forms are (1) black hole attack, (2) flooding attack, (3) data eavesdropping attack, and (4) server key escrow problem. Although the common asymmetric encryption algorithm can be used for identity authentication, because the authentication process is complicated and the key distribution is very inconvenient, people have been looking for an alternative method with efficient authentication capability.

3.2. Traditional IBE Encryption Algorithm. In 1984, Shamir et al. first proposed the concept of identity-based encryption (IBE), but in 2001, IBE was realized by Boneh et al. using bilinear pairings on elliptic curves [25]. However, the current IBE algorithm still has some problems, such as too complicated operation and key escrow. How to improve IBE algorithm and make it really applied in WSN is a hot research topic at present.

The common IBE scheme usually consists of four processes: initialization, private key generation and distribution, encryption, and decryption [26]. Among them, the private key needs to be assigned to the user in advance through the secure channel, while the public key can be generated according to the public information of the user. The workflow of IBE mechanism is shown in Figure 2.

The core of traditional IBE encryption algorithm is bilinear pairing operation, which needs to go through multiple rounds of polynomial iterative process, and the computational complexity is extremely high.

3.3. Improved Identity-Based Encryption Algorithm lIBE. On the basis of studying the encryption structure of traditional IBE algorithm, a scheme IIBE is proposed to solve

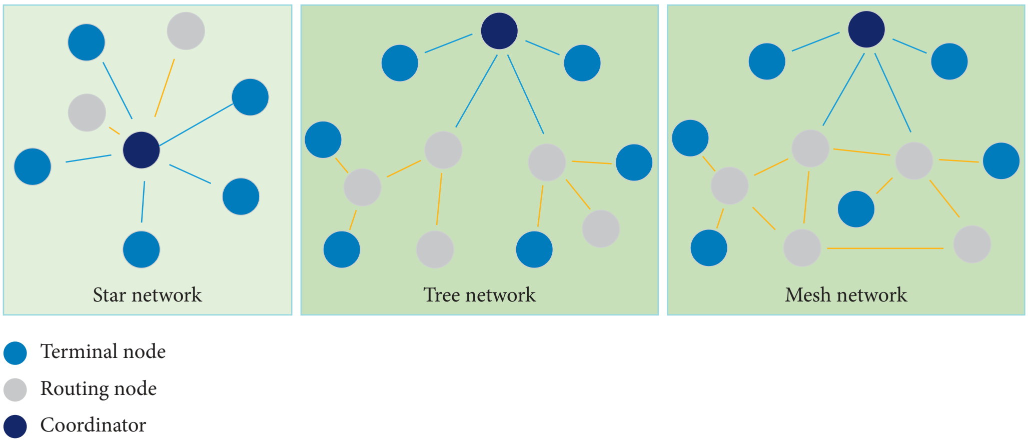

Figure 1: Three topologies of ZigBee network.

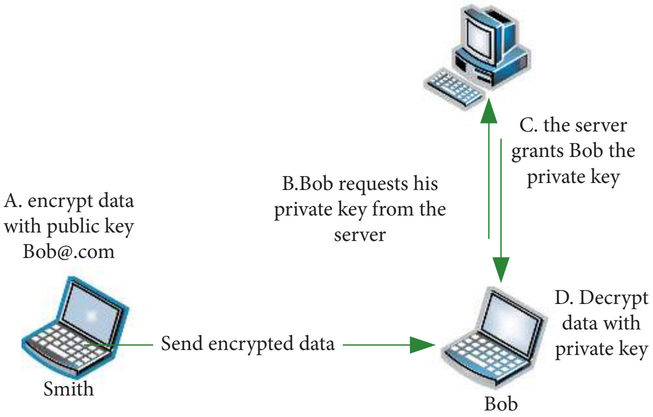
C. the server grants Bob the private key
B.Bob requests his private key from the server
A. encrypt data with public key Bob@.com
Send encrypted data
D. Decrypt data with private key
Smith
Bob

Figure 2: Schematic diagram of IBE workflow.

the above key escrow and revocation problems. The design idea is as follows: the user's private key in the system is divided into two parts, one part is controlled by private key generator (PKG), and the other part is controlled by users themselves. When decrypting, PKG firstly decrypts the received ciphertext with a partial private key and gives the result to the user, and then, the user decrypts it with his own partial private key to obtain the final decrypted plaintext. If a user's key needs to be revoked, PKG does not help the user to decrypt it preliminarily. Because PKG does not master all the private keys, it can avoid the key escrow problem.

IIBE consists of five processes: system initialization, key extraction, public key extraction, encryption, and decryption.

(1) System initialization: the algorithm takes security parameter k as input and returns system parameters *params* and *master-key*. System parameters include the description of plaintext space $\boldsymbol{M}$ and ciphertext space $\boldsymbol{C}$. The algorithm is run by PKG, *params* can be made public, and *master-key* is only known by PKG.

(2) Key extraction: the algorithm takes *params* and a user's *ID* as input and returns the secret value x_{ID} of *ID* and the key X_{SID}. The algorithm can be run by user *ID* or PKG, and the secret value and key are not disclosed after being generated.

(3) Public key extraction: the algorithm takes *params* and the secret value x_{ID} of the user *ID* as input and returns the public key P_{ID} of the user *ID*. The algorithm is run by user *ID*, and the generated public key P_{ID} is made public.

(4) Encryption: the algorithm takes *params*, plaintext $M \in \boldsymbol{M}$, and public key P_{ID} of user *ID* as input. The ciphertext $C \in \boldsymbol{C}$ corresponding to M or the termination symbol "$\perp$" indicates encryption failure, and encryption failure only occurs when the form of public key P_{ID} is incorrect.

(5) Decryption: the algorithm takes *params*, ciphertext C, private key D_{ID}, and key X_{SID} of user *ID* as input and returns plaintext M corresponding to C or termination symbol "$\perp$" to indicate decryption failure.

If ciphertext C is obtained by encryption algorithm (with *params*, P_{ID}, and plaintext M as input), then running decryption algorithm (with *params*, D_{ID}, X_{SID}, and ciphertext C as input) will definitely get correct plaintext M.

The specific operation process of IIBE encryption algorithm initialization and encryption and decryption is shown in Figure 3.

The parameter design of IIBE encryption algorithm is shown in Table 1.

The functions of each parameter are

(1) Public parameter s: the public parameter is randomly generated by the server, not disclosed, only reserved by the server, and used to issue the node private key. However, participates in all encryption, decryption, and authentication operations thereafter [27].

(2) Primitive element P: primitive element belongs to a point in the finite field of elliptic curve, but it plays an extremely important role in IIBE algorithm, so it is an element alone. All points of finite fields can be generated by p.

(3) Public information Q_{bob}: it is some traceable and unchangeable information of nodes.

(4) Public key Q: it is generated by public information Q_{bob}, which is a point on the elliptic curve finite field, and can be generated by the node itself or other nodes according to the public information.

(5) Random parameter r: it is randomly generated by nodes, participating in the ciphertext generation process and participating in the decryption process in the form of rP.

(6) Hash function *Hash*: map a string to a certain point in a finite field [28, 29].

(7) Mapping function number f: convert the string into the corresponding binary code string.

(8) Node private key E: it is generated by the server and assigned to the node.

(9) Original plaintext D: it needs to be mapped to binary code string for encryption and decryption.

3.4. Comparative Analysis of Complexity. We compare IIBE, AES, IBE, and DIOS from two aspects of key security and computational complexity. The comparison results of key security are shown in Table 2.

It can be seen from Table 2 that the key security of the proposed IIBE algorithm is the highest. Then, compare the computational complexity of different algorithms, as shown in Table 3.

It can be seen from Table 3 that, compared with other algorithms, the computational complexity of the proposed IIBE algorithm in system initialization, helping device, and user key update is reduced from O (log N) to o (1), which means that the complexity of the proposed IIBE algorithm is the lowest.

4. Experimental Results and Analysis

4.1. Experimental Setup. In the experiment, the WSN node adopts CC2530 sensor network node of TI (Texas instruments) company [30], which has an enhanced C51 single chip microcomputer and 8k RAM storage space, and is powered by two No.5 batteries [31, 32]. WSN nodes are shown in Figure 4. The actual network topology of IIBE is shown in Figure 5. Settings of WSN network parameters are shown in Table 4.

Ten CC2530 nodes are used for network deployment, and all IIBE nodes in WSN are not set to sleep. All collected data are stored in the MySql database on the server side. Then, it will be tested from three aspects: energy consumption, network communication capability, and security capability.

4.2. Energy Consumption Test. Firstly, the energy consumption of several encryption algorithms is tested. The IIBE algorithm performs node authentication every 30 minutes and key update every two hours in order to approach the actual network deployment situation as much as possible. A total of about 100,000 pieces of actual data were collected by the experimental WSN network, and the fitting curve obtained by sorting out is shown in Figure 6.

The ordinate of Figure 6 shows the average voltage of nodes in the actual distribution network, in volts. The abscissa is the network running time in hours. It can be seen that when the key length is 30 bits, AES encryption supported by CC2530 hardware has the longest duration, and the actual duration of IIBE encryption is about 83 hours, which is more than 10 hours shorter than AES encryption. However, considering that IIBE here sets up internode authentication every half hour, which is different from AES's simple encryption and decryption operation, it can be considered that IIBE can meet the energy consumption requirements when the key length is 30 bits. Generally speaking, the energy consumption of IIBE algorithm is weaker than that of AES, but it can still last for a long time and basically meet the design goals.

4.3. Communication Performance Test. In the experiment, the data that can be effectively counted are the amount of data sent by WSN nodes and received by the server, so compared with the concept of packet loss rate, the concept of data reception rate can describe the actual experiment more accurately. The calculation method of data reception rate [33] is as follows:

$$\mathrm{Pr} = \frac{\sum_{i=0}^{n} n_{(i)\mathrm{receive}}}{\sum_{i=0}^{n} n_{(i)\mathrm{send}}}, \tag{1}$$

where $n_{(i)\,\mathrm{receive}}$ represents the number of data received by the server from ith node and b represents the number of data sent by ith node.

On CC2530 WSN node, the data receiving rates of several methods with 30-bit key are tested, and about 40,000 experimental data are obtained. The statistical fitting curve of the results is shown in Figure 7.

It can be seen from Figure 7 that when the network scale increases, the trend of traffic not only depends on the algorithm itself but also is greatly affected by the network layout. The random distribution method adopted in the experiment makes some nodes close to the coordinator

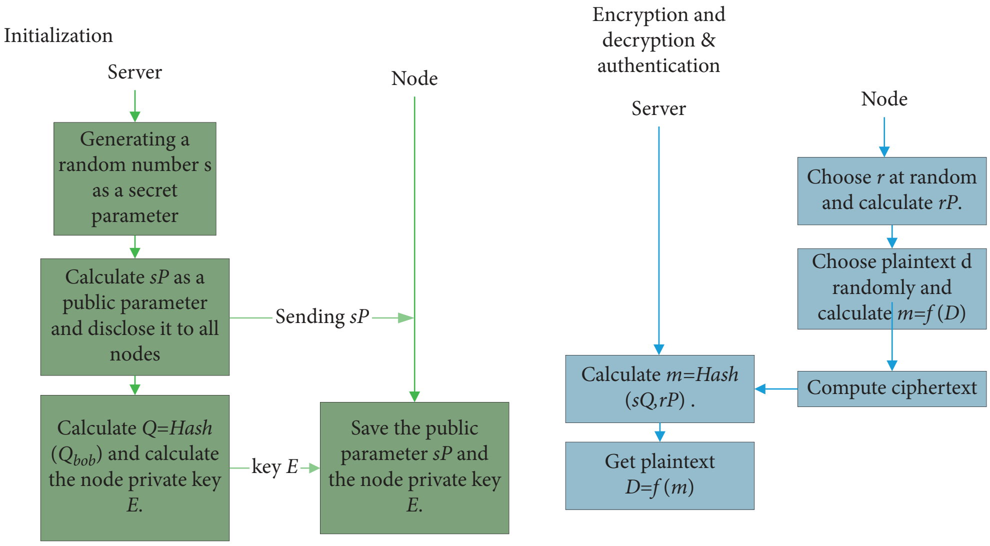
Initialization
Server
Generating a random number s as a secret parameter
Calculate sP as a public parameter and disclose it to all nodes
Calculate Q=$Hash$ (Q_{bob}) and calculate the node private key E.
Node
Sending sP
key E
Save the public parameter sP and the node private key E.
Encryption and decryption & authentication
Server
Node
Choose r at random and calculate rP.
Choose plaintext d randomly and calculate m=f (D)
Compute ciphertext
Calculate m=$Hash$ (sQ,rP) .
Get plaintext D=f (m)

Figure 3: Initialization and encryption and decryption process of IIBE encryption algorithm.

Table 1: Parameter design of IIBE algorithm.

	Common parameters	Primitive element	Public information	Public key	Random parameter	Hash function	Node private key	Mapping function	Original plaintext
Number of parameters	1	1	1	1	1	2	1	2	1
Elemental symbol	s	P	Q_{bob}	Q	r	$Hash$	E	f	D

Table 2: Comparison of key security.

Dataset name	Forward security of key	Backward security of key	Help device key leak
IBE	√		
AES	√		
DIOS	√	√	
IIBE	√	√	√

Table 3: Comparison of computational complexity.

Different stages	IBE	AES	DIOS	IIBE
System initialization	O (log N)	O (log N)	O (1)	O (1)
Help device key update	O (log N)	O (log N)	O (1)	O (1)
User key update	O (log N)	O (log N)	O (1)	O (1)
Help device key refresh	O (log N)	O (log N)	O (log N)	O (1)
User key refresh	O (log N)	O (log N)	O (log N)	O (1)
Encryption	O (log N)	O (log N)	O (log N)	O (log N)
Decode	O (log N)	O (log N)	O (log N)	O (log N)

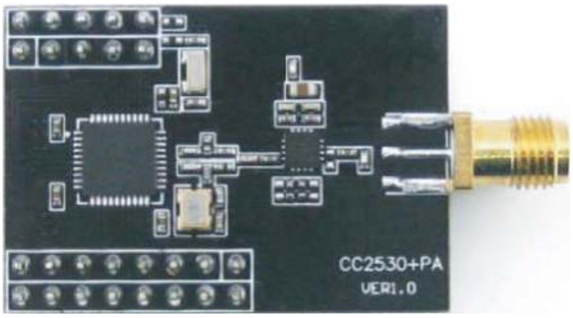

Figure 4: WSN node equipment used in experiment.

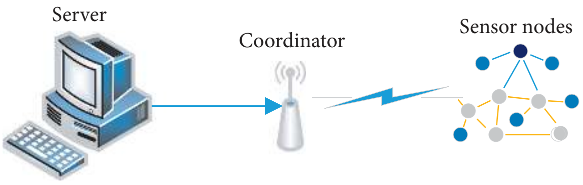

Figure 5: Actual network topology of IIBE.

Table 4: WSN network parameter setting.

Mesh area	Transmission frequency	Initial voltage (V)	Network topology	Longest packet sent in a single time (bit)	Arrangement mode	Key length (bit)	Dormancy
1 km × 1 km	Random (0–60 s)	3.2	Net structure	120	Random	30	No

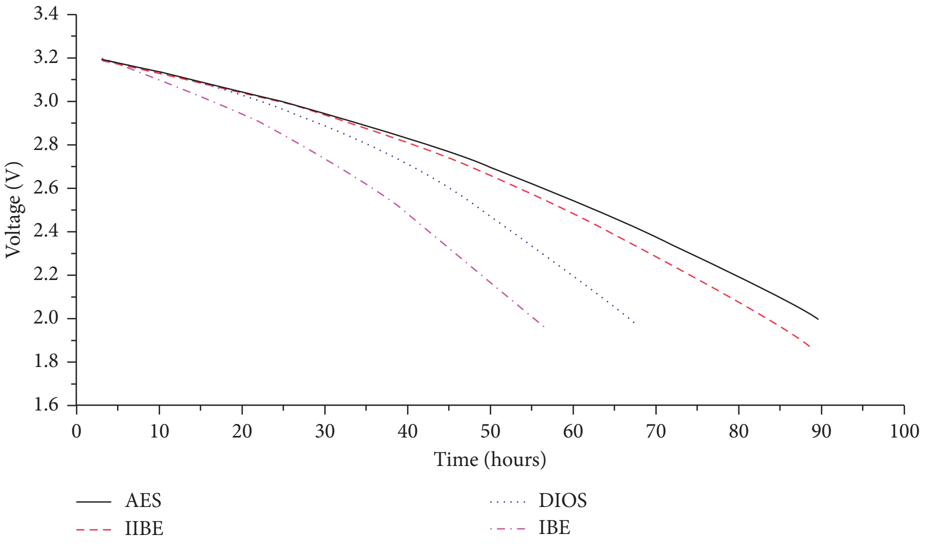

Figure 6: Average voltage trend of WSN nodes.

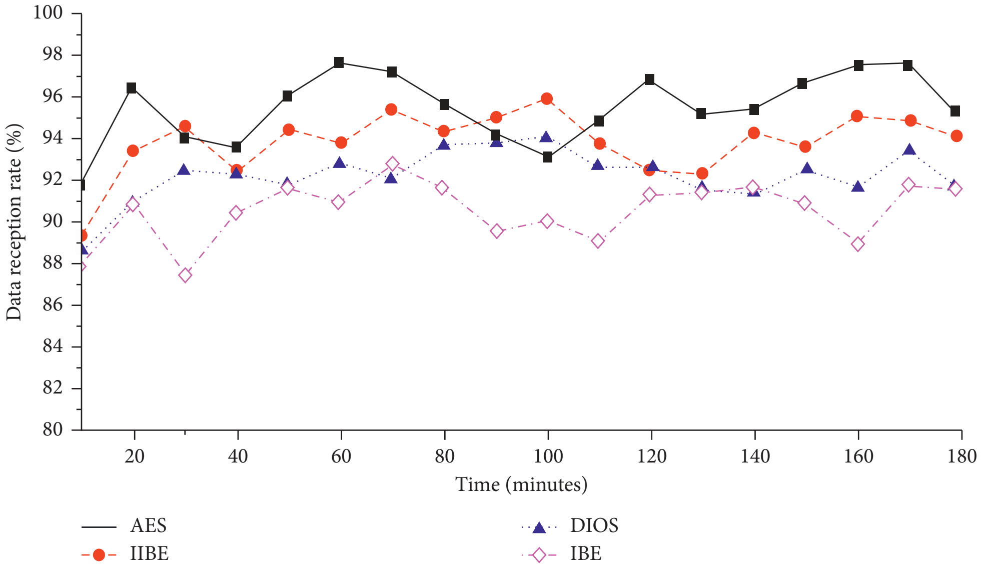

Figure 7: Comparison of network reception rate.

consume more energy and die faster, and the death of these nodes also affects the communication between other nodes and the coordinator. Because IIBE has a key exchange process in the initial stage, there is a large amount of communication in the initial stage. With the steady state of the network, the traffic volume of IIBE network is gradually stable. The algorithms such as DIOS and IBE, which have a large amount of communication, have a low reception rate, while the reception rate of IIBE and AES is higher than that of DIOS, so the reception rate of IIBE algorithm is basically acceptable.

5. Conclusion

Based on the encryption structure of traditional IBE algorithm, this paper proposes a scheme IIBE to solve the above key escrow and revocation problems. The design idea is as follows; the user's private key in the system is divided into two parts: one part is controlled by PKG and the other part is controlled by users themselves. Compared with the traditional public key encryption, this algorithm does not need public key certificates and avoids the management of certificates. Compared with identity-based public key encryption, this algorithm solves the problems of key escrow and key revocation. The whole system test shows that compared with traditional encryption algorithm, the proposed IIBE algorithm has the characteristics of low energy consumption, high encryption strength, and strong authentication capability and is suitable for WSN deployment environment with high security requirements. In the future, the performance of IIBE encryption algorithm will be tested in a larger area of WSN network, and the security of various attacks will be analyzed.

Data Availability

The dataset used in this paper are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. Visconti, R. Ferri, M. Pucciarelli, and E. Venere, "Development and characterization of a solarbased energy harvesting and power management system for a WSN node applied to optimized goods transport and storage," *International Journal on Smart Sensing and Intelligent Systems*, vol. 9, no. 4, pp. 1637–1667, 2016.

[2] S. Bera, S. Misra, S. Kumar Roy, and M. S. Obaidat, "Soft-WSN: software-defined WSN management system for IoT applications," *IEEE Systems Journal*, vol. 12, no. 3, pp. 2074–2081, 2016.

[3] A. N. Alvi, S. H. Bouk, S. H. Ahmed, M. A. Yaqub, M. Sarka, and H. Song, "BEST-MAC: bitmap-assisted efficient and scalable TDMA based WSN MAC protocol for smart cities," *IEEE Access*, vol. 4, no. 1, pp. 312–322, 2016.

[4] X. Yuan, M. Elhoseny, H. K. E-Minir, and A. M. Riad, "A genetic algorithm-based, dynamic clustering method towards improved WSN longevity," *Journal of Network and Systems Management*, vol. 25, no. 1, pp. 1–26, 2016.

[5] J. Su, R. Xu, S. Yu, B. Wang, and J. Wang, "Idle slots skipped mechanism based tag identification algorithm with enhanced collision detection," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 5, pp. 2294–2309, 2020.

[6] C. Zhang, T. Xie, K. Yang et al., "Positioning optimisation based on particle quality prediction in wireless sensor networks," *IET Networks*, vol. 8, no. 2, pp. 107–113, 2019.

[7] J. Su, R. Xu, S. Yu, B. Wang, and J. Wang, "Redundant rule detection for software-defined networking," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 6, pp. 2735–2751, 2020.

[8] A. Mehmood, J. Lloret, and S. Sendra, "A secure and low-energy zone-based wireless sensor networks routing protocol for pollution monitoring," *Wireless Communications and Mobile Computing*, vol. 16, no. 17, pp. 2869–2883, 2016.

[9] M. Elhoseny, H. Elminir, A. Riad, and X. Yuan, "A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic encryption," *Journal of King Saud University - Computer and Information Sciences*, vol. 28, no. 3, pp. 262–275, 2016.

[10] V. Bapat, P. Kale, V. Shinde, N. Deshpande, and A. Shaligram, "WSN application for crop protection to divert animal intrusions in the agricultural land," *Computers and Electronics in Agriculture*, vol. 133, pp. 88–96, 2017.

[11] H. Grichi, O. Mosbahi, M. Khalgui, and Z. Li, "RWiN: new methodology for the development of reconfigurable WSN," *IEEE Transactions on Automation Science and Engineering*, vol. 14, no. 1, pp. 109–125, 2017.

[12] P. Marappan and P. Rodrigues, "An energy efficient routing protocol for correlated data using CL-LEACH in WSN," *Wireless Networks*, vol. 22, no. 4, pp. 1415–1423, 2016.

[13] D. G. Zhang, W. B. Li, S. Liu, and X. D. Zhang, "Novel fusion computing method for bio-medical image of WSN based on spherical coordinate," *Journal of Vibroengineering*, vol. 18, no. 1, pp. 522–538, 2016.

[14] C.-W. Tsai, T.-P. Hong, and G.-N. Shiu, "Metaheuristics for the lifetime of WSN: a review," *IEEE Sensors Journal*, vol. 16, no. 9, pp. 2812–2831, 2016.

[15] Y. K. Joshi and M. Younis, "Restoring connectivity in a resource constrained WSN," *Journal of Network and Computer Applications*, vol. 66, no. 5, pp. 151–165, 2016.

[16] X. Wang, H. Cheng, and Y. Yao, "Addressing-based routing optimization for 6LoWPAN WSN in vehicular scenario," *IEEE Sensors Journal*, vol. 16, no. 10, pp. 3939–3947, 2016.

[17] S. Rohini and L. Daya, "Multi-gateway-based energy holes avoidance routing protocol for WSN," *Informatics*, vol. 3, no. 2, pp. 1–26, 2016.

[18] N. Singh, D. Virmani, and X.-Z. Gao, "A Fuzzy logic-based method to avert intrusions in wireless sensor networks using WSN-DS dataset," *International Journal of Computational Intelligence and Applications*, vol. 19, no. 3, p. 2050018, 2020.

[19] Y. He, Z. Zhang, F. R. Yu et al., "Deep reinforcement learning-based optimization for cache-enabled opportunistic interference alignment wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10433–10445, 2017.

[20] Y. He, N. Zhao, and H. Yin, "Integrated networking, caching, and computing for connected vehicles: a deep reinforcement learning approach," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 44–55, 2018.

[21] K. Muhidul, M. Alam, Y. Moullec, and E. Yaacoub, "Throughput-aware cooperative reinforcement learning for

adaptive resource allocation in device-to-device communication," *Future Internet*, vol. 9, no. 4, pp. 538–548, 2017.

[22] H. Mostafaei, M. U. Chowdhury, and M. S. Obaidat, "Border surveillance with WSN systems in a distributed manner," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1–10, 2018.

[23] N. E. Rachkidy, A. Guitton, and M. Misson, "Avoiding routing loops in a multi-stack WSN," *Journal of Communications*, vol. 8, no. 3, pp. 151–160, 2018.

[24] D. V. Daniela and M. Giovanni, "Spatio-temporal optimization of perishable goods' shelf life by a pro-active WSN-based architecture," *Sensors*, vol. 18, no. 7, p. 2126, 2018.

[25] Y. Melike, V. Güngr, and B. PINar, "Performance analysis of Hamming code for WSN-based smart grid applications," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 26, pp. 125–137, 2018.

[26] T. Xie, C. Zhang, Z. Zhang, and K. Yang, "Utilizing active sensor nodes in smart environments for optimal communication coverage," *IEEE Access*, vol. 7, pp. 11338–11348, 2018.

[27] A. Ahmad and Z. Hanzalek, "An energy efficient schedule for IEEE 802.15.4/ZigBee cluster tree WSN with multiple collision domains and period crossing constraint," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 99, pp. 12–23, 2018.

[28] R. F. Fernandes, M. Almeida, and D. Brandão, "An energy efficient receiver-initiated MAC protocol for low-power WSN," *Wireless Personal Communications*, vol. 100, pp. 1–20, 2018.

[29] H. Liu, J. Shi, J. Li, and C. Liu, "Investigation on the influence caused by shield tunneling: WSN monitoring and numerical simulation," *Advances in Civil Engineering*, vol. 2021, pp. 1–11, 2021.

[30] K. A. Kumar, D. Aju, and K. Keshvi, "An energy efficient and secure mechanism (EES-WSN) in wireless sensor networks for reliable data transmission," *Journal of Engineering Science and Technology Review*, vol. 13, no. 2, pp. 82–91, 2020.

[31] S. Sabah and M. Croock, "Increasing WSN lifetime using clustering and fault tolerance methods," *Iraqi Journal for Electrical And Electronic Engineering*, vol. 17, no. 1, pp. 1–6, 2021.

[32] Z. Zhang, C. Zhang, M. Li, and T. Xie, "Target positioning based on particle centroid drift in large-scale WSNs," *IEEE Access*, vol. 8, pp. 127709–127719, 2020.

[33] L. Wang, C. Zhang, Q. Chen et al., "A communication strategy of proactive nodes based on loop theorem in wireless sensor networks," in *Proceedings of the 2018 Ninth International Conference on Intelligent Control and Information Processing (ICICIP)*, pp. 160–167, IEEE, Wanzhou, China, November 2018.