Internet of Things and Cyber-Physical Systems 1 (2021) 34–44

Contents lists available at ScienceDirect

Internet of Things and Cyber-Physical Systems

journal homepage: www.keaipublishing.com/en/journals/internet-of-things-and-cyber-physical-systems

Sensible and secure IoT communication for digital twins, cyber twins, web twins

Hailin Feng [a,*], Dongliang Chen [b], Haibin Lv [c]

[a] School of Information Engineering, Zhejiang A & F University, Hangzhou, China
[b] Colleage of Computer Science and Technology, Qingdao University, China
[c] North China Sea Offshore Engineering Survey Institute, Ministry of Natural Resources North Sea Bureau, China

ARTICLE INFO

Keywords:
Digital twin
Cyber-physical system
Web twins
IoT communication
Communication security

ABSTRACT

In order to effectively solve the current security problems encountered by smart wireless terminals in the digital twin biological network, to ensure the stable and efficient operation of the wireless communication network. This research aims to reduce the interference attack in the communication network, an interference source location scheme based on Mobile Tracker in the communication process of the Internet of Things (IoT) is designed. Firstly, this paper improves Attribute-Based Encryption (ABE) to meet the security and overhead requirements of digital twin networking communication. The access control policy is used to encrypt a random key, and the symmetric encryption scheme is used to hide the key. In addition, in the proposed interference source location technology, the influence of observation noise is reduced based on the principle of unscented Kalman filter, and the estimated interference source location is modified by the interference source motion model. In order to further evaluate the performance of the method proposed as the interference source, this paper simulates the jamming attack scenario. The Root Mean Square Error (RMSE) value of the proposed algorithm is 0.245 m, which is better than the ErrMin algorithm (0.313 m), and the number of observation nodes of the proposed algorithm is less than half of the ErrMin algorithm. To sum up, satisfactory results can be achieved by taking the Jamming Signal Strength (JSS) information as the observation value and estimating the location of the interference source and other state information based on the untracked Kalman filter algorithm. This research has significant value for the secure communication of the digital twins in the IoT.

1. Introduction

With the development and application of Internet of Things (IoT) technology, the importance of information technology to the modern industry has been enhanced from simply providing the function of a monitoring center to establishing a comprehensive industrial process information framework. In this case, innovative technologies and concepts such as the digital twin emerge, whose essence involves data collection, human-computer interaction, knowledge discovery and generation, intelligent control, and other disciplines [1–3]. In the context of the continuous innovation of various technologies such as embedded sensors, low-power wireless communication, and efficient signal processing, the IoT offer opportunities to connect the physical world and cyberspace. In addition, it can realize fine-grained perception of objects and environment, continuous data collection, comprehensive information fusion, in-depth analysis, and real-time feedback or control of connected targets [4]. According to Gartner's report, there are about 8 billion connected things providing intelligent services in our daily lives, such as assisted living, building monitoring, traffic control, environmental monitoring, and so on.

Based on the widespread application of IoT technology, digital twins have attracted the attention of scholars in recent years. Essentially, the core technology of digital twins is the IoT technology that realizes real-time multi-source data collection. Digital twins represent dynamic digital copies of physical assets, processes, and systems, comprehensively monitoring their entire life cycle [5–7]. In addition, it integrates artificial intelligence and software analysis to create digital simulation models that can be dynamically updated and changed along with physical models. Modern data visualization schemes such as virtual reality and augmented reality can provide more illustrative views. Digital twins can simulate the normal and abnormal behavior of assets. Data-driven models can use data analysis to describe, understand and predict dynamic activities. In

* Corresponding author.
E-mail addresses: hlfeng@zafu.edu.cn (H. Feng), cdlord@qq.com (D. Chen), lvhaibinsoa@gmail.com (H. Lv).

https://doi.org/10.1016/j.iotcps.2021.12.003
Received 7 November 2021; Received in revised form 22 December 2021; Accepted 25 December 2021
Available online 29 December 2021

addition, the application of deep learning technology to the analysis of historical knowledge, data, and events can enable the digital twin model to have the ability to deal with emergencies. In the digital twin, densely networked cameras are deployed at high density to provide seamless surveillance. On the one hand, processing-intensive network video requires the real-time upgrade of computing architecture, such as collaborative edge computing. On the other hand, modern analytical techniques, such as deep learning, to enable IoT devices with limited resources can also relieve the pressure on cloud infrastructure and save network bandwidth [8,9]. Digital twins will create new forms of communication and networking in the future to enable efficient data transmission.

From the perspective of secure communication of IoT based on digital twin, multi-hop wireless sensor networks are usually vulnerable to hacker attacks and active manipulation due to they do not need physical access to cables to participate in the communication. Moreover, the IoT environment covers a large number of different types of heterogeneous networks, which also puts forward higher requirements for the security of information exchange systems based on wireless communication [10,11]. As the support of the information network, intelligent terminals not only provide sensing and control services but also become the entrance for attackers to destroy the IoT. Therefore, this paper discusses the security problems of intelligent wireless terminals in IoT communication for digital twins. Considering that Radio Frequency Identification (RFID) technology can complete massive collection and transmission tasks in the IoT, the security of the IoT-RFID system has also attracted more and more attention. After understanding the security requirements of IoT communication, to reduce the interference attacks in the communication network, this study designed the interference source location scheme based on a mobile tracker in the process of IoT communication, so as to improve the resistance of IoT networks to interference attacks and ensure the communication security.

2. Literature review of secure IoT communication for digital twins

With the support of current IoT technologies such as 5G cellular communications, artificial intelligence, machine learning, and cloud computing, digital twins can be used to understand the real-time status of products and make accurate predictions and assessments of potential failures in the future. With the rapid development of new infrastructure, IoT technology, and other technologies, the communication satellite industry chain is also transforming and developing towards intelligent, digital, and intelligent systems. The integration of digital twin technology uses reasonable data information such as satellite orbit main parameters and communication satellite position information to build a scene of communication satellites operating in orbit, and then reproduce the real-time operation of communication satellites. He et al. (2018) [12] pointed out that digital twins involve data acquisition, human-machine product interconnection, intelligent control, and other steps, and signal processing technology is essential to the above process. Digital twin technology based on signal processing is of great value for comprehensive monitoring and remote diagnosis of the Industrial Internet of Things (IIoT). The IIoT makes distributed intelligent services change with the dynamic industrial environment, thus demonstrating the advantages of Industry 4.0. Sun et al. (2020) [13] constructed a new digital twin-enabled IIoT architecture and proposed a cluster-based asynchronous federated learning framework based on Lyapunov dynamic queue control and deep reinforcement learning theory to improve the learning performance of the system under resource constraints.

In the IoT for Digital Twins, data communication is still the main method of information exchange, and data communication to ensure the security of the IoT has become a very important issue. Xia et al. (2019) [14] studied the power control strategy of intelligent secure communication in the IoT with statistical channel state information, in which the transceiver and attacker have multiple attack types such as eavesdropping, interference, and deception, and proposed a power control strategy based on Q-learning. The goal of flexible choice of action of IoT nodes is realized, and its performance optimization in security is ensured. Raza et al. (2017) [15] implemented Constrained Application Protocol (CoAP) for resource-constrained IoT devices and the cloud and used the original public key and certificate-based asymmetric encryption technology to protect resources from IoT devices. The implementation method of packet transport layer security protocol is supplemented for resource receiving IoT devices. In information communication on the IoT, the encryption scheme has been proved to be suitable for the secure transmission of all kinds of information. Naresh et al. (2017) [16] proposed a new identity-based online/offline signcryption scheme for providing secure communication services between IoT devices, gateways, and servers. This mechanism reduces the online computing time by performing more operations in the offline sign-on phase.

Integrating existing studies, the IoT is in a critical stage of development, however, there is no systematic research on the communication security of the IoT based on digital twins. In order to fill this research gap, this paper protects the integrity and confidentiality of communication on the basis of considering the high efficiency of IoT communication. In addition, the problem that attackers tamper with the information transmission data of the IoT through wireless interfaces is studied, and the interference source locating scheme based on the mobile tracker is proposed to ensure the communication security of the IoT.

3. Secure IoT communication algorithm based on digital twin

3.1. IoT system architecture for digital twins

The IoT is making digital twins more diversified and complicated due to the connected devices and sensors that make up the IoT accurately collecting all kinds of data needed to build the digital twin. In the IIoT, digital twins can be composed of equipment on the production line to provide information for proactive repair and maintenance methods. Digital twinning can even operate at the whole city level, enabling local authorities and governments to run smoother, more efficient, and smarter public services through virtual replication of interconnected systems [17–19]. Taking IIoT-based product manufacturing as an example, digital twins for interconnected products can achieve more reactive problem solutions through remote diagnosis. And the historical data and actual data recorded in the digital twin are used to find the correct solution. Fig. 1 shows the main process of applying digital twins to complete product production in IIoT manufacturing. During the planning phase, the data is allowed to simulate asset performance and evaluate risks in detail, supplementing and enhancing traditional reliability engineering methods. The digital twin of the connected asset can serve as an integration point for the various stakeholders working with the asset. This not only includes owner/operator operations and maintenance staff but also external service providers, insurance companies, and other financial service providers. The main process of product evaluation by digital twin in the IIoT is shown in Fig. 2.

Data is the key to the development and application of digital twin technology, and the basic requirements of digital twin data acquisition are real-time, distributed, and fault tolerance. The accurate control of digital twin needs to be based on sampling data, so the delay of information processing has higher requirements, and the time synchronization between multiple sensor units in the system must be ensured. The offline data warehouse is mainly based on the big data technology of Hadoop ecological components and is mainly based on distributed computing in computing to improve the operational performance of data [20,21]. The real-time data warehouse is roughly the same as the offline data warehouse, and its application advantage lies in ensuring real-time data. The service mapping model oriented to the digital twin network provides data required for modeling through a unified data service interface, as well as various services such as data search, batch service, and historical rollback. The key to meeting the compatibility and

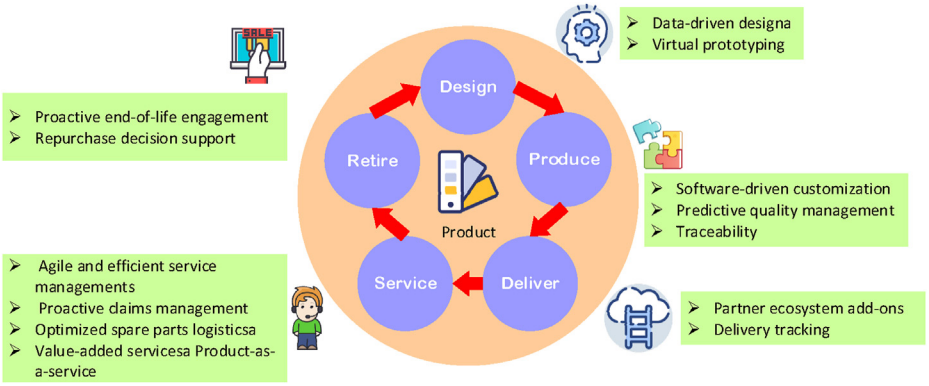


Fig. 1. The main process of product production by digital twin in the IIoT.

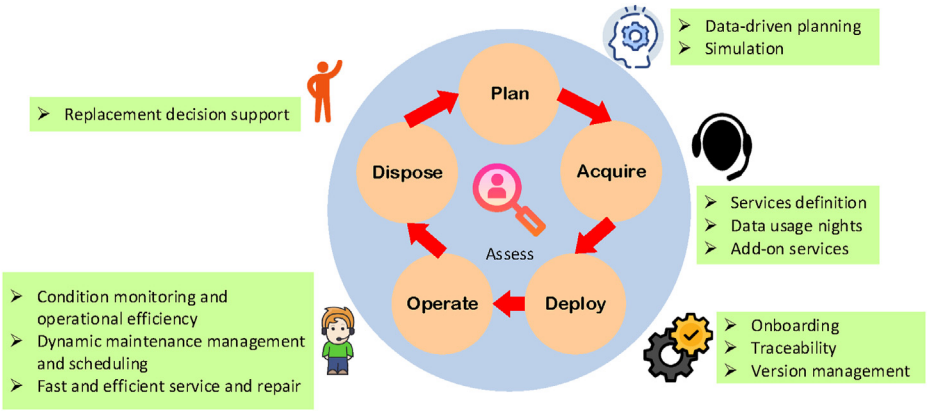


Fig. 2. The main process of product evaluation by digital twin in the IIoT.

scalability of the digital twin network lies in the standardized interface and protocol system. The data acquisition interface is responsible for completing the data acquisition of the twin network layer data sharing warehouse, and the control issuing interface is responsible for issuing the control instructions after the simulation verification of the service mapping model to the physical network layer. With the development of the network scale, there are more and more upper-layer application systems, and the number of lower-layer physical network elements is gradually increasing, resulting in a rapid increase in the actual number of network interfaces. In order to quickly introduce and integrate new applications and new functions, it is necessary to adopt a unified and highly scalable standardized interface in the design of the twin network interface.

3.2. IoT secure communication based on ciphertext attribute-based encryption scheme

In the digital twin network that contains a large amount of data, it is more vulnerable to massive attacks such as eavesdropping, deception, and denial of service. Traditional internet systems reduce attacks by relying on encryption and data authentication methods at the link layer, network layer, transport layer, or application layer. Although some of these solutions are suitable for the IoT, due to the inherent limited

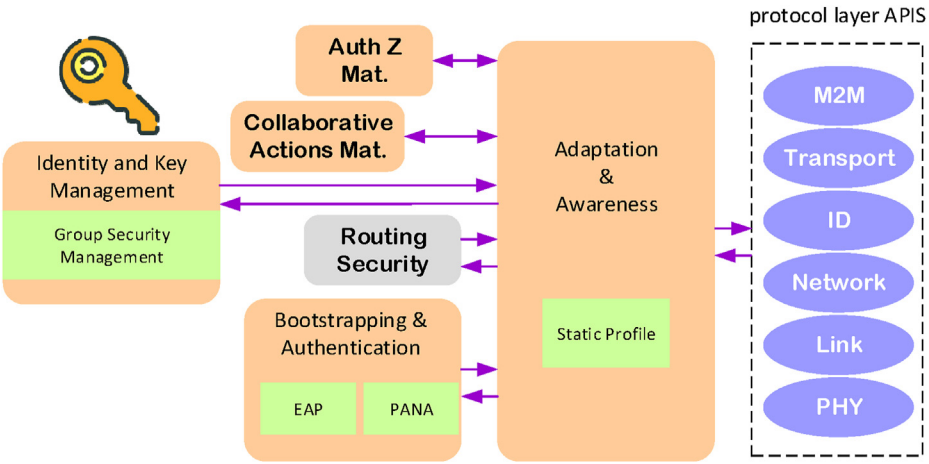


Fig. 3. IoT security protocol architecture.

processing and communication capabilities of the IoT devices, this hinders the use of the aforementioned security kits to a certain extent. The IoT security protocol architecture constructed is shown in Fig. 3. The functional security module is on the left, tightly integrated with the communication stack on the right. Authentication is critical for secure IoT communication and is likely to be the first operation a node performs when joining a new network, using an authentication server in the network access protocol. After successful validation, a higher-level security association can be established between the node and the associated access control agent. Negotiation is required before security associations are established to ensure that agreement on the cipher suite can be reached between the relevant nodes and access control.

In many cases, when users encrypt sensitive data, specific access control policies must be established for who can decrypt this data. Those who own confidential data must be able to choose an access strategy based on specific knowledge of the underlying data. And this person may not know the exact identity of others who have access to the data, but their identity can be described by attributes. Traditional access control is implemented by using trusted servers to store data locally. However, due to the emergence of more and more data are stored in distributed and cross-server, traditional methods are becoming more and more difficult to ensure data security. In this paper, we improve Attribute-Based Encryption (ABE) to meet the security requirements and overhead requirements in IoT communication for digital twins.

In the basic ABE scheme, the central authority (*CA*), data owner (*DO*), and data user (*DU*) are involved in three parties [22–24]. The system initialization algorithm (*Setup*) is executed by *CA*, first enter the security parameters (k) and the user attribute domain (U), and output the system master key (*MK*) and public parameter *params*:

$$(k, U) \rightarrow (MK, params) \tag{1}$$

The key generation algorithm *KeyGen* is also executed by *CA*, input *MK* and a permission index X, and output the corresponding key sk_X:

$$KeyGen(MK, X) \rightarrow sk_X \tag{2}$$

The encryption algorithm (*Enc*) is executed by *DO* , input *params* and a message m to be encrypted and a ciphertext index Y, finally output the corresponding ciphertext CT_Y:

$$Enc(params, m, Y) \rightarrow CT_Y \tag{3}$$

Decryption algorithm (*Dec*) is executed by *DU*, input system common parameters *params*, and CT_Y, and output plaintext M:

$$Dec(params, sk_X, CT_Y) \rightarrow M \tag{4}$$

If ABE is implemented based on a key policy, X and Y represent an access structure and a set of attributes, respectively. If ABE is implemented based on a ciphertext policy, X and Y represent an attribute set and an access structure, respectively.

On the basis of ABE, Ciphertext Policy Attribute-Based Encryption (CP-ABE) is proposed, and its application is shown in Fig. 4. The ciphertext corresponds to an access structure and the key corresponds to a set of attributes. Decryption is conditional that only the attributes in the attribute collection satisfy this access structure. This design is closer to the actual application scenario, which can pretend that each user obtains the key from the attribute organization according to their own conditions or attributes, and then the encryptor formulates the access control to the message.

The attributes owned by a user may be managed by multiple organizations in actual situations. Therefore, in order to effectively solve the key distribution problem in multi-organizations, this paper proposes a new type of Multiple Properties Fine-Grained Access Control (MPFAC). The scheme is constructed based on a prime order group, and the computational efficiency is higher than the composite order group. Moreover, the various agencies are only responsible for distributing keys of the attributes they manage, and they are not affected by each other.

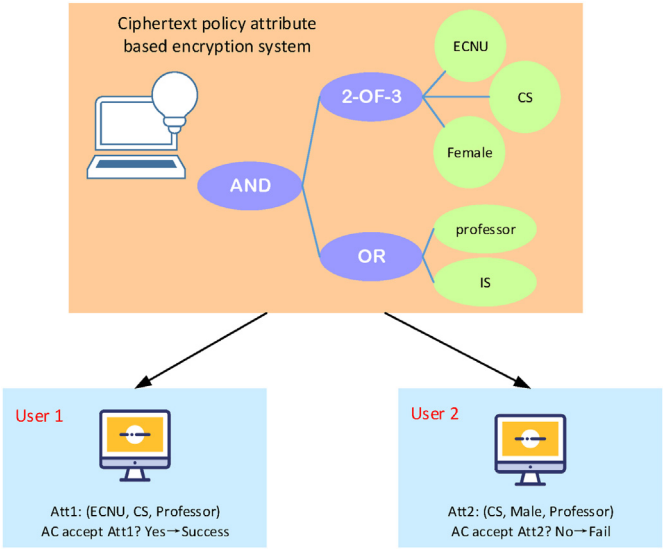


Fig. 4. The application mode of CP-ABE scheme.

The new plan includes four participants: Attribute Authority (AA_i), Cloud Server (*CS*), Data Owner (*DO*), and Data User (*DU*). Each AA_i manages some of the attributes of *DU* and generates corresponding cloud server private keys for these attributes; *CS* is responsible for storing encrypted data securely and managing each user's private key; *DO* uses its own access policy to The data is encrypted and uploaded to *CS*. *DU* requests data from *CS*, and if the attributes of *DU* satisfy the access structure, it returns to the corresponding place to decrypt the ciphertext, and then *DU* uses the private key to decrypt the part of the decrypted ciphertext. In this scheme, an access control strategy is used to encrypt a random key R, while the real M uses a symmetric encryption scheme to hide the key.

3.3. The algorithm for locating interference sources in the IoT based on mobile trackers

The basic idea of the Catch the Jammer (CJ) algorithm includes two aspects: First, when a sensor node in the network detects a jamming attack, the edge node at the edge of the jamming area immediately broadcasts packets to its one-hop neighbor node outside the jamming area. The neighbor nodes that receive the packet communicate with each other, share the location information of the interfering node, and enable the interference source locating algorithm. The other part is the localization process, CJ algorithm firstly calculates the convex shell of the disturbed node-set, and then finds the minimum covering circle of the convex shell. The pseudo-code implementation of the CJ algorithm is shown in Fig. 5.

As for the problem that wireless communication between intelligent terminals of the IoT is prone to interference attacks, this paper starts from the terminal network layer and locates interference sources to minimize interference attacks and provide active protection for the communication security of the IoT. First, the distance between the interfered observation node and the interference source is estimated based on the Jamming Signal Strength (JSS) of the observation node [25,26]. On this basis, in the technical framework of the mobile platform, interference sources can be automatically tracked and located to improve the efficiency of interference elimination. Fig. 6 shows the workflow of the interference source location.

JSS covers the distance information between the observation node and the interference source. Assuming that the position of the interference source N_J at time t is $x_J = [x_J, y_J]^T$, there is an observation node N_i at the position $x_i = [x_i, y_i]^T$, and the signal strength of the interference source observed by N_i is:

Input: $Q=\{(X_1,Y_1),(X_2,Y_2),...(X_n,Y_n)\}$

Output: $\hat{Q}_J$ (The estimated location of the interferer)

1. Calculate the convex hull: $CH(Q)=\{P_1,P_2,...P_m\}$

2. Find the diameter l of $CH(Q)$, with endpoints P_i and P_j.

3. Judge: *if* $d(O,P_v)<r$

4. **then** $\hat{Q}_J=O$

5. **else go to** Step 6

6. **end if**

7. Calculate $d(P_u,P_iP_j)$

8. Find the k corresponding to the maximum value (Satisfy $d(P_u,P_iP_j)=\max\{d(P_u,P_iP_j)\}_{u=1,2...m}$)

9. Find the intersection point of the vertical line of the diameter P_iP_j and P_iP_k line segment O_1

10. Judge: *if* $d(O_1,P_v)<r_1$

11. **then** $\hat{Q}_J=O_1$

12. **else if** $P_{k'}$ and P_k are on the same side of diameter P_iP_j.

13. **while** $(k')\neq\phi$ **do**

14. **Replace** $P_{k'}$ **with** P_k; **return** Step 9

15. **end while**

16. **end**

17. **else if** $P_{k'}$ and P_k are on the opposite side of diameter P_iP_j

18. then find the $P_{k''}$ that satisfies $\min(\angle P_iP_kP_{k'})$

19. Pass points $P_{k'}$, $P_{k''}$, and P_i to make a circle, the center of the circle is O_2.

20. $\hat{Q}_J=O_2$

21. **end**

22. **end if**

23. end

Fig. 5. Pseudo-code implementation of CJ algorithm for interference source location.

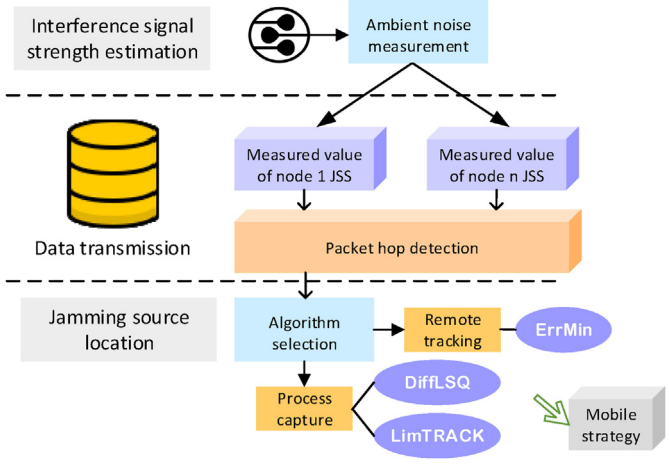


Fig. 6. Workflow of interference source location.

$$P_{r_i}=P_0-10\eta\log_{10}\left(\frac{d_i}{d_0}\right)+X_{\sigma_i} \tag{5}$$

$$d_i=\|x_i-x_J\|_2=\sqrt{(x_i-x_J)^2+(y_i-y_J)^2} \tag{6}$$

where P_0 represents the reference signal strength measured by the interference source at the reference distance d_0, and d_0 is taken as 1 m. X_σ represents the Gaussian zero-mean noise caused by the shadow effect; η is the path loss index; the distance between the observation node N_i and the interference source N_J is represented by d_i.

In the above equation, the reference signal strength P_0 and the interference source location $x_J=[x_J,y_J]^T$ are unknown quantities. Therefore, $\theta=[x_J^T,P_0]^T$ can be used as the parameter vector to be estimated. Assuming that the set of observation nodes is $N=\{N_1,N_2...N_i\}$, each node can obtain the corresponding observation information, which is represented as:

$$P_{r_1}=P_0-10\eta\log_{10}d_1+X_{\sigma_1} \tag{7}$$

$$P_{r_i}=P_0-10\eta\log_{10}d_i+X_{\sigma_i} \tag{8}$$

X_{σ_1} is Gaussian noise with independent and identical distribution, so for the JSS observation value P_{r_1} from i observation nodes, the probability density function is:

$$f(P_{r_1}|\mu_i,\sigma)=\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left\{-\frac{(x-\mu_i)^2}{2\sigma^2}\right\} \tag{9}$$

$$\mu_i=P_0-10\eta\log_{10}d_i \tag{10}$$

For the independent ISS observation value P_{r_1} of i observation node, the joint probability density function is:

$$f(P_{r_1}|\theta,\sigma)=f(P_{r_1}|\theta,\sigma)f(P_{r_2}|\theta,\sigma)..f(P_{r_i}|\theta,\sigma) \tag{11}$$

The likelihood function can be defined as:

$$L(\theta,\sigma;P_r)=f(P_r|\theta,\sigma)=\prod_{N_i\in N}f(P_{r_j}|\theta,\sigma) \tag{12}$$

Take the logarithmic form of equation (12) to obtain the logarithmic likelihood, which is expressed as:

$$L(\theta,\sigma;P_r)=\sum_{N_i\in N}\ln(P_{r_j}|\theta,\sigma) \tag{13}$$

The maximum likelihood estimation θ_{ML} of θ can be described as an optimization problem:

$$\theta_{ML}=\arg\max_{\theta}\ln L(\theta,\sigma;P_r) \tag{14}$$

The log likelihood function can be represented as:

$$L(\theta,\sigma;P_r)=-\frac{i}{2}\ln(2\pi)-\frac{i}{2}\ln(\sigma^2)-\frac{1}{2\sigma^2}\sum_{N_i\in N}(P_{r_i}-P_0+10\eta\log_{10}d_i)^2 \tag{15}$$

From equation (15), the maximum likelihood estimate θ_{ML} of θ can be given, represented as:

$$\theta_{ML}=\arg\max_{\theta}\sum_{N_i\in N}(P_{r_i}-P_0+10\eta\log_{10}d_i)^2 \tag{16}$$

Since the interference source in the IoT has the characteristics of omnidirectionality, but its location is within the area formed by the observation node, the optimized search space can be constrained to obtain:

$$\theta_{ML} = \underset{\theta}{\operatorname{argmax}} \sum_{N_i \in N} (P_{r_i} - P_0 + 10\eta \log_{10} d_i)^2 \quad x_{\min} \le x_J \le x_{\max} \quad y_{\min} \le y_J \le y_{\max} \tag{17}$$

where $x_{\min}$ and $x_{\max}$ are the minimum and maximum coordinate values of the observation node axis respectively, $y_{\min}$ and $y_{\max}$ are the minimum and maximum coordinate values of the observation node axis respectively.

Based on the Kalman filter algorithm, this paper describes the positional relationship of the interference source at different times. First, let be the state of the interference source at the first sampling moment after discretization, and the motion of the interference source can be described as:

$$x_n = f(x_n - 1) + w_n \tag{18}$$

where w_n refers to model noise with Gaussian distribution.

The JSS observation function given in this paper corresponds to the observation equation defined by the Kalman filter algorithm:

$$z_n = h(x_n + v_n) \tag{19}$$

where v_n is the measurement noise with Gaussian distribution.

If the observation sequence is z_n after the measurement of JSS by n observation nodes at time n, it can be concluded that:

$$z_i^n = P_0 - 10\eta \log_{10}\left(d_i^n\right) + v_n \tag{20}$$

$$d_n^i = \sqrt{\left(x_J^n - x_i^n\right)^2 + \left(y_J^n - y_i^n\right)^2} \tag{21}$$

where z_i^n refers to the observation value given by node N_i.

The interference source location technology mentioned in this paper mainly includes two stages, namely the remote tracking and the close acquisition stage. Remote tracking means that the JSS measurement value can be obtained from the boundary node when the tracker does not enter the interference area. The key to remote tracking is to drive the tracker as close to the interference source as possible in a short time [27–29]. For close acquisition, the tracker can directly collect measurement values from the interfered node to locate the interference source in real-time [30]. Before designing the positioning algorithm for the remote stage, this paper firstly improves the optimization objective function and transforms it into an optimization problem in which only the position of the interference source is used as the estimated parameter. The mean value of the JSS observation data P_r can be obtained:

$$\overline{P_r} = P_0 - \frac{1}{i} \sum_{j=1}^{i} 10\eta \log_{10} d_i + X \tag{22}$$

Base on the nonlinear least square method, the estimation of the interference source position can be obtained:

$$x_J = \underset{x_J}{\operatorname{argmin}} \sum_{N_i \in N} \left(P_{r_i} + 10\eta \log_{10} d_i - \overline{P_r} - \frac{1}{i} \sum_{j=1}^{i} 10\eta \log_{10} d_i \right)^2 \tag{23}$$

when:

$$P_{J_i} = P_{r_i} + 10\eta \log_{10} d_i \tag{24}$$

Simplified optimization objective function can be obtained:

$$x_J = \underset{x_J}{\operatorname{argmin}} \left(P_{J_i} - \overline{P}_{J_i} \right) \tag{25}$$

In general, the positioning algorithm of remote tracking is based on the observation data obtained from the collection of boundary nodes [31–33]. Finally, an intelligent optimization algorithm is used to calculate the value of the optimization objective function for each location in the search interval to obtain the estimated value of the interference source location. The algorithm requires that the number of observation nodes is greater than 3 to ensure that the measurement value is obtained from a sufficient number of observation nodes.

The positioning algorithm for the close acquisition includes a static algorithm and a dynamic algorithm, where the static algorithm is used to generate the initial state of the dynamic algorithm. In the static algorithm, if the tracker can collect JSS from more than two observation nodes, the JSS measurement value measured by the observation node N_i is P_{r_i}. The distance estimate from the observing node to the interference source can be calculated:

$$d_i = 10^{\frac{P_{J_i} - P_{r_i}}{10\eta}} \tag{26}$$

The following equation can be obtained:

$$\left(x_J - x_i\right)^2 + \left(y_J - y_i\right)^2 = d_i^2 \tag{27}$$

Estimate the position of the interference source at time t by the least square method:

$$x_J = \left| x_{J_t}, y_{J_t} \right|^T = (A^T A)^{-1} A^T b \tag{28}$$

$$A = \begin{pmatrix} x_1 - x_n & y_1 - y_n \\ \cdots & \\ x_{n-1} - x_n & y_{n-1} - y_n \end{pmatrix} \tag{29}$$

$$b = \frac{1}{2} \begin{pmatrix} \left(x_1^2 - x_n^2\right) + \left(y_1^2 - y_n^2\right) - \left(d_{1,t}^2 - d_{n,t}^2\right) \\ \cdots \\ \left(x_{n-1}^2 - x_n^2\right) + \left(y_{n-1}^2 - y_n^2\right) - \left(d_{n-1,t}^2 - d_{n,t}^2\right) \end{pmatrix} \tag{30}$$

In the dynamic algorithm, the unscented Kalman filter achieves high positioning accuracy. The minimum sample point set σ of each mean represents the estimate of the true state, and the output of the unscented Kalman filter is the weighted average of all points σ.

State initialization:

$$\begin{aligned} x_0 &= E[x_0] \\ P_0 &= E\left[\left(x_0 - x_0 \right) \left(x_0 - x_0 \right)^T \right] \end{aligned} \tag{31}$$

x_0 is the initial state value of the interference source obtained by the remote algorithm, and P_0 represents the initial error covariance matrix.

Calculate point σ:

$$\begin{cases} x_{0,t-1} = x_{t-1} & \omega_0 = \lambda \Big/ (L + \lambda) \\ x_{i,t-1} = x_{t-1} + \left(\sqrt{(L+\lambda) P_{t-1}} \right)_i & \omega_i = 0.5 \Big/ (L + \lambda) \\ x_{i+L,t-1} = x_{t-1} + \left(\sqrt{(L+\lambda) P_{t-1}} \right)_i & \omega_{i+L} = 0.5 \Big/ (L + \lambda) \end{cases} \tag{32}$$

where L is the dimension of state x, λ is the parameter used to adjust ω, and P_{t-1} represents the posterior error covariance matrix at $t - 1$.

The output of the unscented Kalman filter is a posterior estimate $x_t = [x_t, y_t, v_{x,t}, v_{y,t}]^T$ of the interference source state and an error covariance matrix P_t of the posterior estimate.

To sum up, the interference source location technology proposed in this paper is based on the principle of the unscented Kalman filter to reduce the impact of observation noise. The interference source motion model can realize the correction of the estimated location of interference sources, and further improve the positioning accuracy of the model for interference sources in the IoT.

3.4. Application analysis of IoT security communication scheme

In order to better evaluate the performance of the MPFAC scheme in the secure communication of the IoT mentioned in this paper, the attribute-based encryption scheme is implemented based on the Jpbc library and the Jama library. Both the client and the cloud server use the Win 7 operating system, the CPU is Intel Core i5-8400 @ 2.80 GHz, running memory with 8 GB. In the testing process, 10 attribute institutions (each containing 10 attributes) are selected, and the two independent variables of user attributes and strategy attributes are tested separately. When the number of user attributes is increased from 10 to 100 with a step length of 10, the number of policy attributes is set to 100; and when the number of policy attributes is increased from 10 to 100 with a step length of 10, the number of user attributes is set to 2. The comparison schemes selected in this paper are ABE, CP-ABE, Discretionary Access Control (DAC), and Attribute-Based Access Control (ABAC). The storage cost and calculation cost of the system are counted to verify the correctness. The improved effectiveness of the ciphertext attribute-based encryption scheme. Further, the attribute-based encryption scheme MPFAC proposed here is compared with the traditional encryption scheme proposed by Fan et al. (2019) [34].

In order to further evaluate the performance of the interference source determination method proposed in this paper and verify the feasibility of interference source location based on JSS measurement values, this paper simulates interference attack scenarios, as shown in Fig. 7. A mobile interference source and 13 observation nodes were built with wireless measurement nodes, and the deployment was completed in a 25×30 m^2 site. The interference source consists of a mobile robot and a wireless measurement node that moves between positions [3,0] and [−3,0]. The proposed algorithm is implemented in MATLAB, and the interference source location is estimated based on the JSS measurement value with a timestamp. The feasibility of the algorithm is evaluated by the difference between the estimated value and the actual location. Absolute Error (Error), Root Mean Square Error (RMSE), and Cumulative Distribution Function (CDF) were used to evaluate the performance of the algorithm. The comparison algorithm used in the experimental verification is to find the optimal solution for four intelligent optimization algorithms include Genetic Algorithm (GA), Multi-directional Search (MDS), Generalized Pattern Search (GPS), Generalized pattern Search (GMS), and Simulated Anneal (SA), respectively.

4. Results and discussion

4.1. Performance analysis of the ciphertext attribute-based encryption scheme for IoT communication

This paper first compares the storage overhead of different attribute-based encryption schemes, and the results are shown in Fig. 8. With the linear growth of attributes, the storage overhead is very low. In the case of 100 attributes, even the ciphertext length does not exceed 1500 bytes.

Fig. 7. Jamming source attack scenario.

Obviously, the MPFAC scheme proposed in this paper is lower than the other four schemes in key length, ciphertext length, and trap gate length. Therefore, the storage cost of this scheme is lower and it is more suitable for lightweight data access.

Fig. 9 shows the comparison of the computational cost of different attribute-based encryption schemes. It can be seen that with the increase in the number of user attributes, the cost of encryption calculation and search calculation for all schemes basically increases linearly. The MPFAC scheme proposed in this paper shows obvious performance advantages in the decryption calculation overhead, and the time overhead of the decryption process has nothing to do with the number of user attributes. The number of user attributes has a small impact on the encryption time of the MPFAC scheme, which enables low-performance clients to complete encryption. This also means that any user can be not only a data uploader but also a data user.

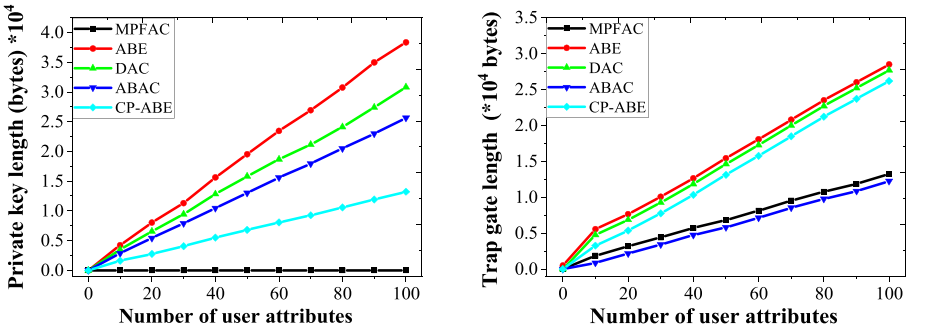
In the attribute-based encryption mechanism, the access policy and private key are related to user attributes. The scheme proposed here not only ensures almost the same computing efficiency, but also protects the user's privacy and adds verifiability. Through the online/offline mechanism, the scheme enables the mobile terminal with low performance to act as data uploader and data user. Compared with the existing schemes, this scheme has more comprehensive nature and stronger expansibility.

The attribute-based encryption scheme MPFAC proposed here is compared with the traditional encryption scheme. Fig. 10 presents the comparison results of key generation time of different schemes. When the number of access policy attributes is set to 4, 8, 12, and 16, with the increase of the number of attributes, the proposed scheme needs the blockchain consensus network for secret sharing when generating the user's private key, so the time cost of key generation here is about 70 ms higher than that in the scheme of Fan et al. When the number of access policy attributes is set to 4 and the number of users is 1, 2, 4, and 6 respectively, with the increase of the number of users, the key time of this scheme has obvious advantages over the traditional encryption scheme. Since the user private key SK of the scheme proposed by Fan et al. is generated by the key center, the key of this scheme is generated by the key escrow center SK1, blockchain consensus network, and user SK2. Finally, the user obtains the final SK, so it has obvious advantages in large-scale distributed applications.

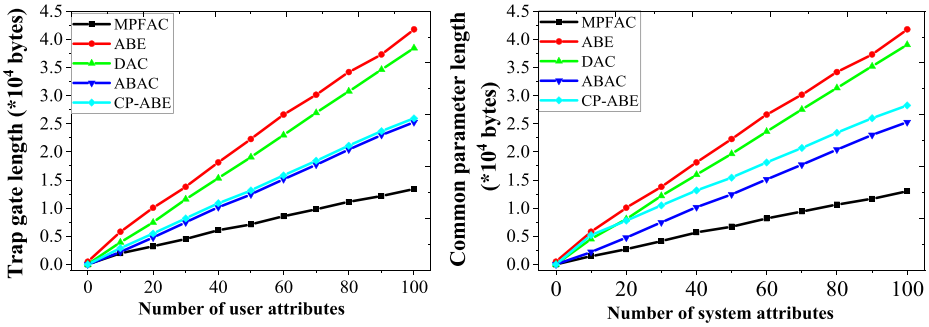
4.2. IoT communication interference source as algorithm performance evaluation

Fig. 11 shows the positioning accuracy of the positioning algorithm in the remote tracking phase of the proposed scheme. Fig. 11(a) shows the trend of the absolute error of the algorithm over time, and Fig. 11(b) shows the cumulative distribution function of the estimated error. It can be seen that the estimation error of the algorithm proposed in this paper is always less than 1 m, and is better than the positioning accuracy of the other four search algorithms.

Regarding the interference source as the positioning algorithm in the close acquisition stage of the scheme, the number of observation nodes is reduced, thus reducing the communication interference received in the process of tracking the interference source. The minimum and maximum observation nodes are 2 and 6, respectively. The positioning algorithm proposed in this paper is compared with ErrMin of the existing interference source positioning algorithm. The number of observation nodes of the ErrMin algorithm is fixed to nodes 1 to 8. The results show that the RMSE of the algorithm proposed in this paper is 0.245 m, which is better than the 0.313 m of the ErrMin algorithm, and the number of observation nodes of the positioning algorithm in this paper is less than half of the ErrMin algorithm. Furthermore, this paper evaluates the influence of path loss error η on the accuracy of the algorithm in the close acquisition process, and the results are shown in Fig. 12. The value of η is set between 2.0 and 3.0. It can be seen that the value of η has little effect on the close algorithm, and the RMSE value of the positioning algorithm proposed in this paper is always better than the ErrMin algorithm. When the value of

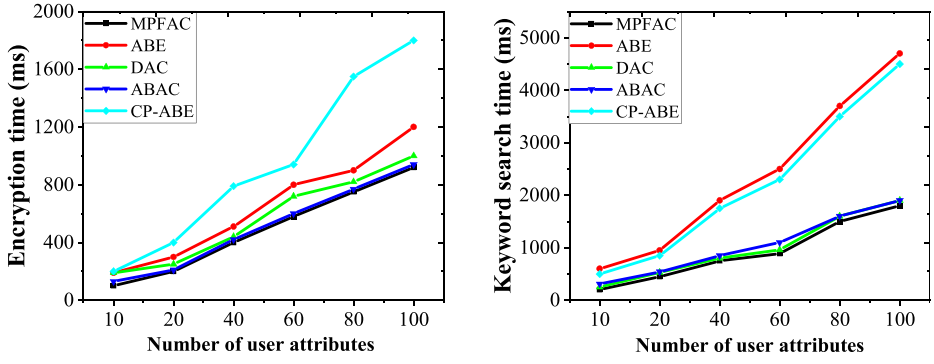


(a) Private key length comparison (b) Ciphertext length comparison

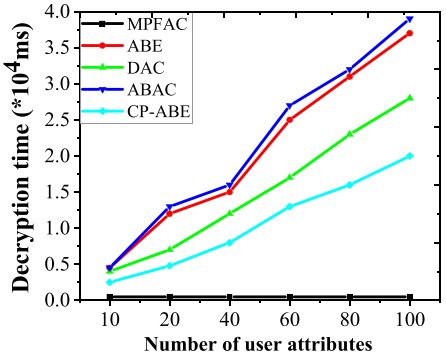


(c) Trap gate length comparison (d) Common parameter length comparison

Fig. 8. Comparison of storage overhead of different attribute-based encryption schemes.



(a) Encryption time (b) Keyword search time



(c) Decryption time

Fig. 9. Comparison of computational overhead of different attribute-based encryption schemes.

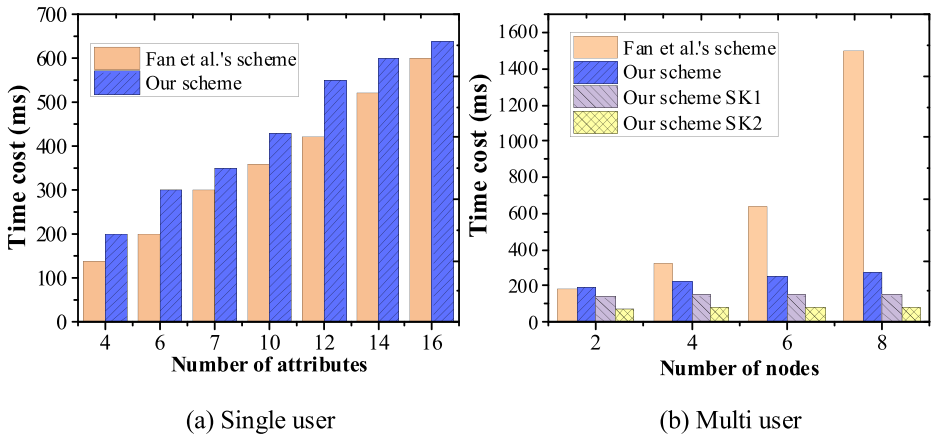


Fig. 10. Comparison of key generation time.

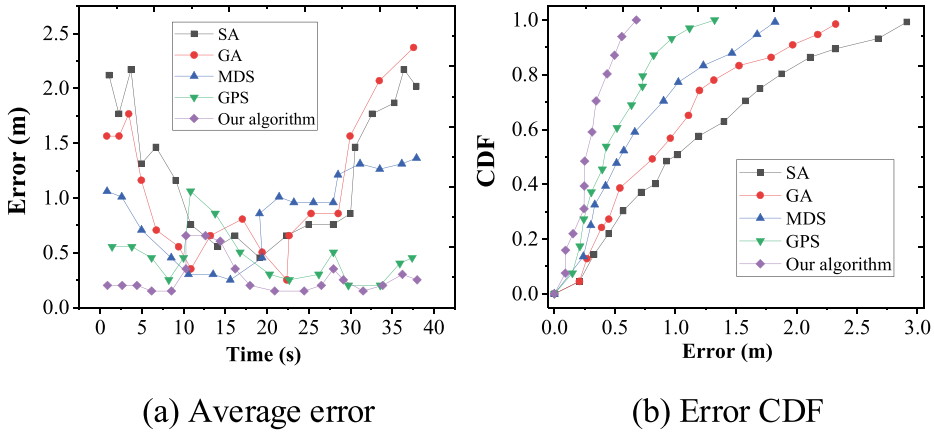


Fig. 11. Comparison of positioning algorithm errors in remote tracking stage.

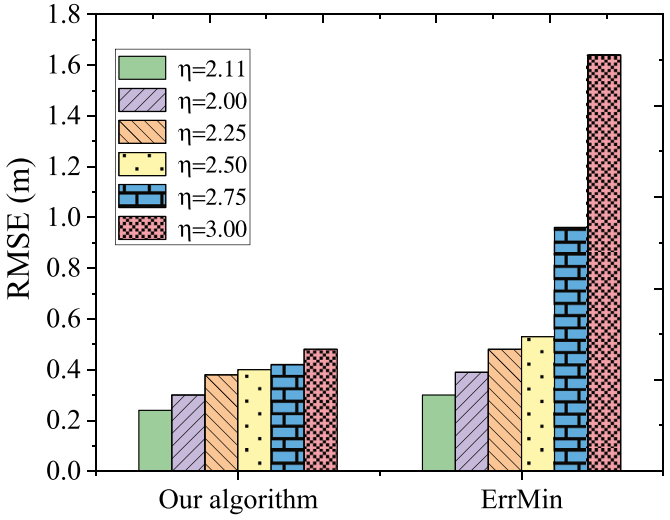


Fig. 12. The influence of path loss error on the accuracy of the algorithm.

η is greater than 2.5, the RMSE value of the ErrMin algorithm has increased significantly. The reason is that the positioning algorithm in this paper uses the principle of unscented Kalman filtering, and the estimated value is the weighted value of the model output and the observation, so the influence of the error on the result during the weighting process has been significantly reduced.

Fig. 13 shows the impact of IoT node density and shadow effects on the accuracy of different positioning algorithms. The distance between nodes is defined as 10–40 m, and the RMSE value was calculated as the algorithm. It can be seen that as the distance between nodes increases, the number of observation nodes in the interference area decreases, and the performance of the algorithm is reduced to varying degrees, but the performance of the algorithm in this paper is always better than other algorithms. The results show that the RMSE values of different algorithms are still greater than zero when there is no shadow effect. With the increase of σ value, the RMSE value of different algorithms increases, and in any case, the positioning algorithm proposed in this paper achieves better performance.

Fig. 14 shows the relationship between the time and speed for the tracker to capture the interference source on four different paths that the interference source moves. Define a capture range of 10 m and set the speed ratio range of the tracker and the interference source to 1.0–2.0. The maximum speed of the interference source was 10 m/s, and the speed range of the tracker was set to 10–20 m/s. The initial positions of the interference sources in the four paths are (100,100), (100,100), (0,200), and (0,200) respectively. When the value of the ratio is 1.0, since the distance between the interference source and the tracker will not decrease with time, the tracker cannot capture. The capture rate of all routes will increase with the increase of the speed ratio, and the capture time will decrease with the increase of the speed ratio. When the value of the ratio is greater than 1.5, the capture rates of the three routes are all greater than 75%.

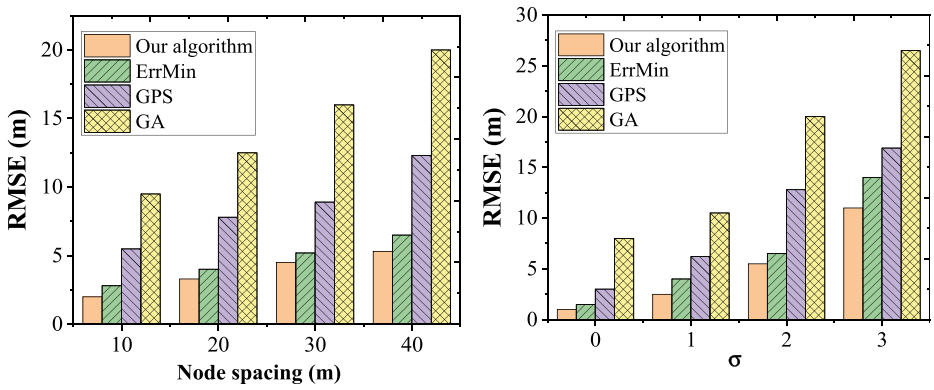


Fig. 13. The influence of node density and shadow effect on different positioning accuracy.

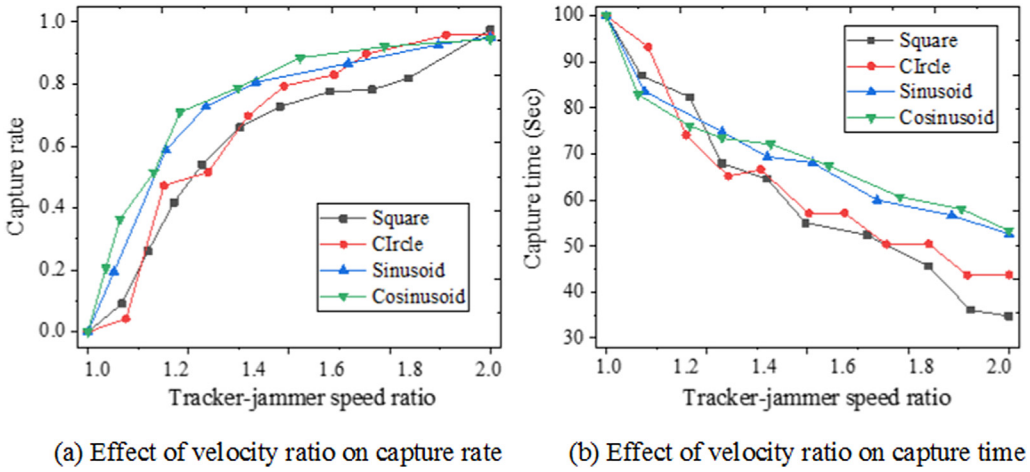


Fig. 14. The influence of node density and shadow effect on different positioning accuracy.

5. Conclusions

The IoT is making digital twinning more diverse and complicated because the connected devices and sensors that make up the IoT accurately collect all kinds of data needed to build the digital twin. While information sharing and exchange bring convenience, information security has gradually become one of the key issues affecting data transmission. This study focuses on the problem that attackers tamper with the information transmission data of the IoT through wireless interfaces, and proposes an interference source location scheme based on a mobile tracker to ensure the communication security of the IoT. The distance between the interfered observation node and the interference source is estimated based on JSS, and the automatic tracking and locating of the interference source is realized under the technical framework of the mobile platform.

This paper proposes to deploy trackers with autonomous mobility capabilities in the IoT network, through the interference signal strength observation information obtained from the node terminal, so as to locate the interference source existing in the network. To ensure the positioning accuracy in the wireless communication environment of the IoT, the interference source positioning technology proposed in this paper is based on the unscented Kalman filter to reduce the influence of observation noise. In addition, the motion interference source model is constructed based on the interactive multi-model framework, and the estimated position is modified to improve the positioning accuracy. Simulation experiments have also confirmed that in any case, the RMSE value of the positioning algorithm proposed in this paper is lower than other algorithms and shows better performance. However, there are still some shortcomings in this paper, the proposed method is based on ranging and cannot cope with the situation where the attacker constantly changes the signal strength of the interference source. In the future study, more subtle reactive interference sources can be discussed, considering the situation where multiple attackers conduct interference attacks at the same time.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] C. Fan, C. Zhang, A. Yahja, et al., Disaster City Digital Twin: a vision for integrating artificial and human intelligence for disaster management[J], Int. J. Inf. Manag. 56 (2021), 102049.
[2] P.D.U. Coronado, R. Lynn, W. Louhichi, et al., Part data integration in the Shop Floor Digital Twin: mobile and cloud technologies to enable a manufacturing execution system[J], J. Manuf. Syst. 48 (2018) 25–33.
[3] Z. Cunbo, J. Liu, H. Xiong, Digital twin-based smart production management and control framework for the complex product assembly shop-floor[J], Int. J. Adv. Manuf. Technol. 96 (1–4) (2018) 1149–1163.
[4] K. Mao, G. Srivastava, R.M. Parizi, et al., Multi-source fusion for weak target images in the Industrial Internet of Things[J], Comput. Commun. 173 (2021) 150–159.
[5] L. Yujun, Z. Zhichang, W. Wei, et al., Digital twin product lifecycle system dedicated to the constant velocity joint[J], Comput. Electr. Eng. 93 (2021), 107264.

[6] L. Yujun, Z. Zhichang, W. Wei, et al., Digital twin product lifecycle system dedicated to the constant velocity joint[J], Comput. Electr. Eng. 93 (2021), 107264.
[7] J. Yu, Y. Song, D. Tang, et al., A Digital Twin approach based on nonparametric Bayesian network for complex system health monitoring[J], J. Manuf. Syst. 58 (2021) 293–304.
[8] J. Lee, M. Azamfar, J. Singh, et al., Integration of digital twin and deep learning in cyber-physical systems: towards smart manufacturing[J], IET Collab. Intell. Manuf. 2 (1) (2020) 34–36.
[9] Q. Wang, W. Jiao, Y.M. Zhang, Deep learning-empowered digital twin for visualized weld joint growth monitoring and penetration control[J], J. Manuf. Syst. 57 (2020) 429–439.
[10] A. Burg, A. Chattopadhyay, K.Y. Lam, Wireless communication and security issues for cyber–physical systems and the Internet-of-Things[J], Proc. IEEE 106 (1) (2017) 38–60.
[11] K. Gai, K.K.R. Choo, M. Qiu, et al., Privacy-preserving content-oriented wireless communication in internet-of-things[J], IEEE Internet Things J. 5 (4) (2018) 3059–3067.
[12] Y. He, J. Guo, X. Zheng, From surveillance to digital twin: challenges and recent advances of signal processing for industrial internet of things[J], IEEE Signal Process. Mag. 35 (5) (2018) 120–129.
[13] W. Sun, S. Lei, L. Wang, et al., Adaptive federated learning and digital twin for industrial internet of things[J], IEEE Trans. Ind. Inf. 17 (8) (2020) 5605–5614.
[14] J. Xia, Y. Xu, D. Deng, et al., Intelligent secure communication for Internet of Things with statistical channel state information of attacker[J], IEEE Access 7 (2019) 144481–144488.
[15] S. Raza, T. Helgason, P. Papadimitratos, et al., SecureSense: end-to-end secure communication architecture for the cloud-connected Internet of Things[J], Future Generat. Comput. Syst. 77 (2017) 40–51.
[16] V.S. Naresh, S. Reddi, S. Kumari, et al., Practical identity based online/off-line signcryption scheme for secure communication in internet of things[J], IEEE Access 9 (2021) 21267–21278.
[17] G. Schrotter, C. Hürzeler, The digital twin of the city of Zurich for urban planning [J], PFG J. Photogram. Remote Sens. Geoinf. Sci. 88 (1) (2020) 99–112.
[18] C. Zhuang, J. Liu, H. Xiong, et al., Connotation, architecture and trends of product digital twin[J], Comput. Integr. Manuf. Syst. 23 (4) (2017) 753–768.
[19] X. Li, J. Cao, Z. Liu, et al., Sustainable business model based on digital twin platform network: the inspiration from haier's case study in China[J], Sustainability 12 (3) (2020) 936.
[20] D. Yao, Y. Chen, Design and implementation of log data analysis management system based on Hadoop[J], J. Inf. Hiding Priv. Protect. 2 (2) (2020) 59.
[21] N. Mollaei, S.H. Mousavi, Application of a Hadoop-based distributed system for offline processing of power quality disturbances[J], Int. J. Power Electron. Drive Syst. 8 (2) (2017) 695.
[22] P. Hu, H. Gao, A key-policy attribute-based encryption scheme for general circuit from bilinear maps[J], Int. J. Netw. Secur. 19 (5) (2017) 704–710.
[23] M. Han, M. Zhu, P. Cheng, et al., Implementing an efficient secure attribute-based encryption system for IoV using association rules[J], Symmetry 13 (7) (2021) 1177.
[24] S. Karthi, S. Prabu, Spatial data storage and retrieval in cloud computing environments using attribute based encryption algorithm[J], Int. J. Internet Technol. Secur. Trans. 9 (1–2) (2019) 163–183.
[25] W. Aldosari, M. Zohdy, Localizing jammer in an indoor environment by estimating signal strength and Kalman filter[J], Wireless Eng. Technol. 9 (2) (2018) 20.
[26] S.M. Mariappan, S. Selvakumar, A novel location pinpointed anti-jammer with knowledged estimated localizer for secured data transmission in mobile wireless sensor network[J], Wireless Pers. Commun. 118 (4) (2021) 2073–2094.
[27] J. Shao, B. Du, C. Wu, et al., Tracking objects from satellite videos: a velocity feature based correlation filter[J], IEEE Trans. Geosci. Rem. Sens. 57 (10) (2019) 7860–7871.
[28] B.A. Raut, R. Jackson, M. Picel, et al., An adaptive tracking algorithm for convection in simulated and remote sensing data[J], J. Appl. Meteorol. Climatol. 60 (4) (2021) 513–526.
[29] A. Sclocco, S.J.Y. Ong, S.Y. Pyay Aung, et al., Integrating real-time data analysis into automatic tracking of social insects[J], R. Soc. Open Sci. 8 (3) (2021), 202033.
[30] A. Sorriento, M.B. Porfido, S. Mazzoleni, et al., Optical and electromagnetic tracking systems for biomedical applications: a critical review on potentialities and limitations[J], IEEE Rev. Biomed. Eng. 13 (2019) 212–232.
[31] S.G. Pease, P.P. Conway, A.A. West, Hybrid ToF and RSSI real-time semantic tracking with an adaptive industrial internet of things architecture[J], J. Netw. Comput. Appl. 99 (2017) 98–109.
[32] A.A. Aziz, L. Ginting, D. Setiawan, et al., Battery-less location tracking for Internet of Things: simultaneous wireless power transfer and positioning[J], IEEE Internet Things J. 6 (5) (2019) 9147–9164.
[33] Y. Yang, M. Zhong, H. Yao, et al., Internet of things for smart ports: technologies and challenges[J], IEEE Instrum. Meas. Mag. 21 (1) (2018) 34–43.
[34] Y. Fan, X. Lin, W. Liang, et al., TraceChain: A Blockchain-Based Scheme to Protect Data Confidentiality and traceability[J], Practice and Experience, Software, 2019.