Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

Blockchain based trusted execution environment architecture analysis for multi - source data fusion scenario

Nan Yang[1], Li Yang[1], Xingzhou Du[1], Xunyi Guo[1], Fanke Meng[2,3] and Yuwen Zhang[4*]

Abstract

Multi-source data fusion techniques are widely applied in dynamic target detection scenarios, such as target situational awareness, radar signal resolution, and feature fusion labeling. Currently, techniques including clustering, neural networks, Bayesian analysis, and machine learning have been applied to improve the success rate of multi-source data fusion in terms of interference data noise reduction. The research on data tampering prevention of multiple data sources is mainly based on the data distributed authentication technology. The research on performing data fusion process in a trusted execution environment is mainly based on cryptography and codec technology. This paper focuses on the technical application architecture that can effectively improve the comprehensive efficiency of multi-source data fusion processing under the constraints of business scenarios. Accordingly, this paper proposes a trusted execution environment architecture based on blockchain technology for multi-source data fusion scenarios. It integrates the strategy of trusted data source data verification in blockchain smart contracts into the typical multi-source data fusion application architecture. After comparison tests in a simulation environment, the trusted execution environment architecture based on blockchain technology has shown considerable improvements in fusion success rate with limited performance cost.

Keywords Multi-source data fusion, Trusted execation environment, Blockchain, Sensing and computing

Introduction

Multi-source data fusion is a technology that integrates information obtained from various sources through investigation and analysis. It uses relevant means to evaluate the information uniformly and obtain a unified view of the data. In short, multi-source datafusion is to provide users with a unified view of multiple information sources [1]. This technology involves the intersection of artificial intelligence, signal processing, fuzzy mathematics and other disciplines. The multi-source has an extensive scope. Sources include tangible data such as sensors, databases, environmental information, images, and intangible data such as models and estimates.

This concept was first proposed in the 1970s to meet the requirements of military Command, Control, Communications, and Intelligence (C3I) system construction. Chen et al. [2] provides commanders with decision-making information by detecting, associating, tracking, estimating and integrating the targets concerned through spatially distributed multi-source data and spatiotemporal sampling of various sensors. At present, this technology is widely used in transportation engineering [3], environmental science [4] and engineering, medical treatment and other fields [5].

*Correspondence:
Yuwen Zhang
zhangyuwen@caict.ac.cn
[1] CSSC Systems Engineering Research Institute, Beijing, China
[2] Xi'an University of Post and Telecommunicaiton, Xi'an, China
[3] Tianjin Yinyuan Information Technology Co., Ltd., Tianjin, China
[4] China Academy of Information and Communications Technology, Beijing, China

The multi radar data fusion [6] mentioned in this paper refers to the effective data fusion of track data from multiple radars for the same target, so that the original data can be combined to form a new fusion track data with higher accuracy. There are many methods for multi radar track/point fusion in engineering practice, such as weighted fusion [7], Kalman filtering [8], Bayes probability theory [9], D-S evidence theory [10], artificial neural network [11], and other information fusion technologies. These methods mainly focus on the spatio-temporal registration of multi-source data in the process of data fusion, which involves converting the multi-source data to a spatio-temporal unified standard time scale without error, and then extracting and fusing the information technology after preprocessing. Thus, these methods can solve many issues such as the sudden fluctuation of radar detection in complex actual environment and the jitter of radar track position, the inconsistency of multiple radars reporting the position of the same target, and the inconsistency of multiple radars judging the movement trend of the same target are solved. However, it is unable to deal with the multi radar data that is attacked by the network and tampered maliciously during the fusion process. Such attacks can cause errors in the fusion of data, resulting in discrepancies between the calculated output and the original data. This can lead to reduced accuracy, which can compromise the reliability and security of the system. Additionally, incorrect decision-making information may be provided to commanders, which can have serious consequences.

To solve and suppress this problem, the multi-source radar data can be fused using the computational power of blockchain technology [12]. On the one hand, blockchain is a distributed data storage technology based on Cryptography, which can ensure the traceability of the whole chain data; On the other hand, the decentralized nature of blockchain ensures the security of data during the fusion process [13]. This allows for deep support of communication, awareness, and computation functions, which can work together to achieve an integrated system of communication, sensing, and computing, thus promoting the enhancement of the comprehensive system capability. A smart contract [14] is a significant feature of the blockchain 2.0 era. It enables the encapsulation, verification, and execution of complex distributed behaviors through conditional and responsive computing procedures that run on a distributed ledger. In addition, the programmed setting without human participation also makes the whole communication, sensing and computing supply chain more secure.

The main contributions are summarized as follows:

- Propose to encapsulate multi-source data processing architecture with blockchain business processing architecture
- Design a TEE business model for trusted computing environment supporting concurrent collaboration
- Testing performance for typical business scenarios to prove technical feasibility and effectiveness

The remainder is provided as follows. The related background is in Section "Related background". The system architecture design is shown in Section "System architecture design". Simulation and results are provided in Section "Simulation and results". Section "Numerical results" introduces the numerical results, and the paper is concluded in Section "Conclusion". Finally, our future work is given in Section "Future work".

Related background

In the military field, data fusion is to fuse the data acquired by multiple sensors, so as to obtain more accurate and useful information than a single sensor. The purpose of data fusion is to improve the accuracy of results based on the complementarity of multi-source data. Additionally, it can also eliminate the outliers and noises of the results according to the redundancy of data.

Currently, as shown in Fig. 1, in the military field, multi-source data fusion has been widely used for the detection of air targets.

This involves the use of multiple radars/satellites to detect targets simultaneously, employing a series of data fusion methods to achieve more accurate target track information than a single radar. However, during the detection process, the radar is vulnerable to attack by the enemy, and the detection results of the radar will have errors through information jamming. This will lead to large deviations in the results of multi-source information fusion and affect the operational decision.

With the deepening understanding of blockchain, the application of blockchain has gradually expanded from the financial field to the military field. Many countries and regions such as the United States, Russia, and NATO have accelerated the military application of blockchain. Blockchain technology has great application value in command and control, combat support, and military resource management [15]. Among them, the blockchain provides an effective guarantee for military data security and security protection [16]. The tamper proof [17] and traceability [18] of the

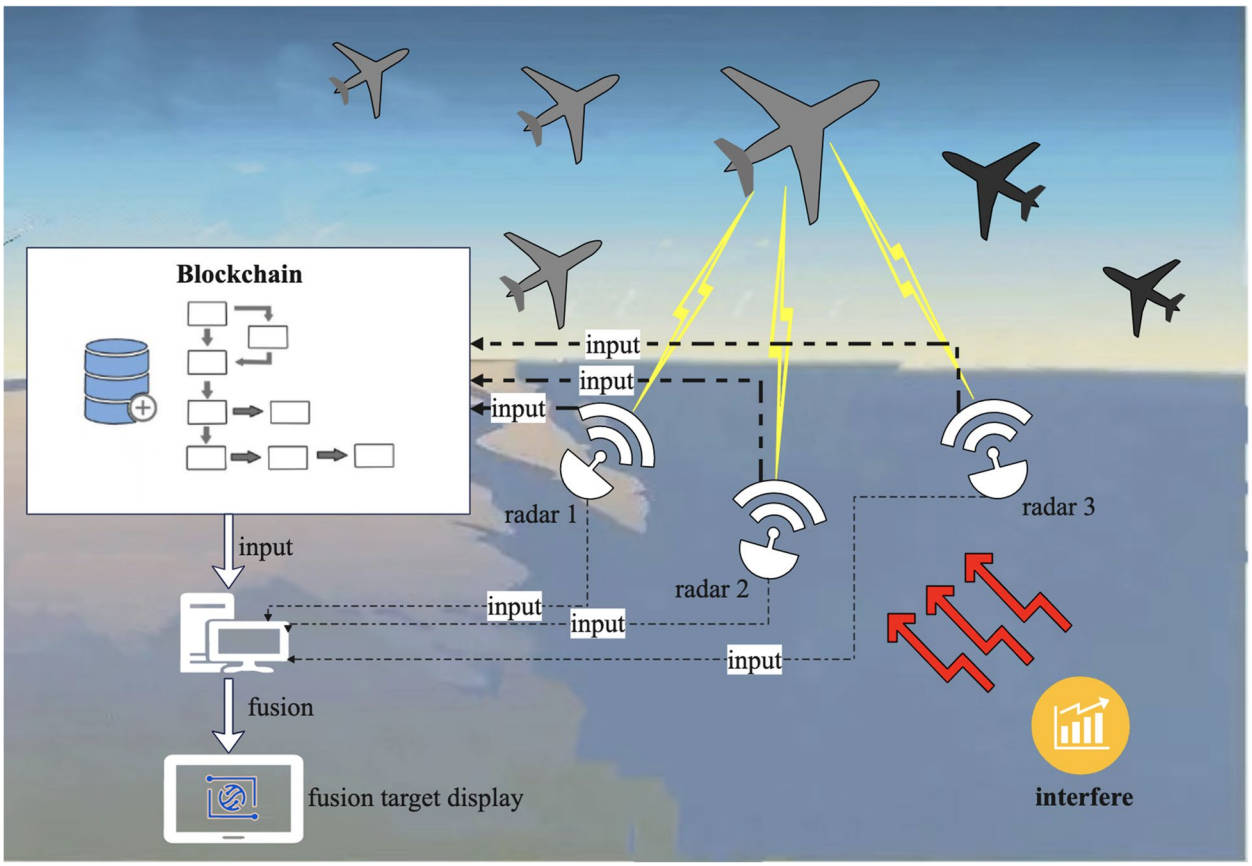

Fig. 1 Radar multi-source data fusion scenario based on blockchain

blockchain can effectively improve the reliability, credibility and availability [19] of data. Radar plays a crucial role in target detection. If radar detection data is written into the blockchain and encrypted and verified by a hash algorithm, it can effectively prevent the data from being attacked and tampered by the enemy in transmission, ensure the data security of multi-source information fusion input source, improve the accurate acquisition of target tracks, and thus improve the combat decision-making and combat capability. However, it's important to note that while ensuring data security, blockchain will also increase the consumption of resources and performance.

System architecture design

The section mainly explains the architecture design of the system, describes the concepts related to blockchain and data security, and introduces the methods and processes for radar multi-source data fusion based on blockchain.

Blockchain and data security

Blockchain is a decentralized distributed data management technology based on distributed database through data encryption and consensus mechanism [20]. Logically, blockchain forms a chain-like structure, where each node is a block information, and the block stores the transaction information. The basic data structure of the blockchain consists of two parts: the intra block structure and the inter block chain structure. As is shown in Fig. 2, the block includes the block header and the block body. The block header information is the metadata of the block, which is used to verify the block and establish associations with its predecessor and successor blocks. The block body information is the sequence of transactions. In the blockchain structure, a block is only considered valid if its signature meets verification requirements.

As shown in Fig. 3, blockchain divides data into different blocks, and each block is linked to the back of the previous block through specific information, forming a chain structure.

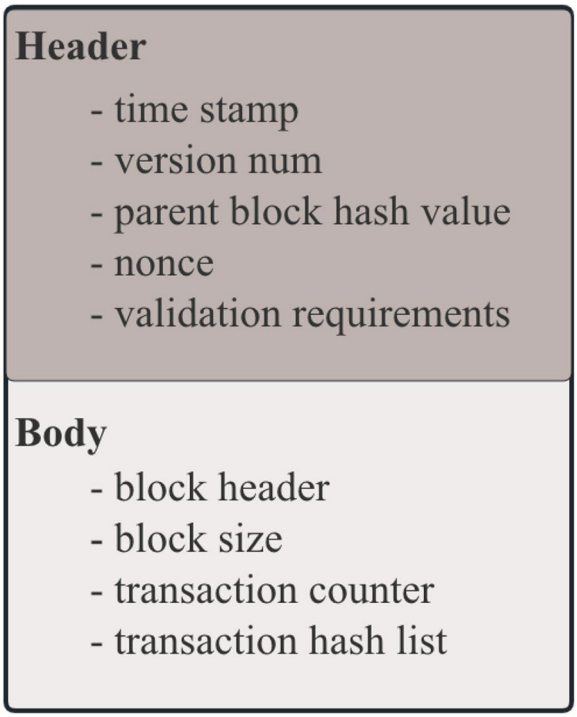

Fig. 2 The Block structure

The block header of each block contains the hash value of the previous block, which is obtained by calculating the hash function of the block header of the previous block. The blocks are linked to each other by hash values to form a chain. Blockchain can ensure data security and credibility, which mainly depends on its blockchain structure. Each block has a timestamp, uses the hash encryption information of the previous block, and verifies each block in the chain. On the basis of block chain, by combining with distributed storage and Byzantine fault-tolerant mechanism [21], data can be effectively guaranteed to be tamper proof and traceable.

The low-level distributed bookkeeping is oriented to resources such as computation and storage, while high-level distributed bookkeeping is oriented to "trusted". Token is the technical form of "trusted", which is built based on certain cryptographic algorithm, not easy to be enumerated and easily verified, in order to achieve the security of technical scope. When a transaction is sent to the blockchain network (also known as "broadcast"), the legitimacy of the transaction needs to be checked first. An important part of the transaction legitimacy verification is to check the validity of the signature, which must be generated by the private key and is unique for each transaction and will not be reused. "Trusted" is mainly achieved through blockchain-based data verification, which is anti-error to illegal data. The received data is signed and the signature is verified during data fusion.

Blockchain and radar multi-source data fusion

Radar data fusion [22] is divided into centralized processing and distributed processing. In this paper, distributed data processing is adopted. As shown in Fig. 4, each radar detects the target, and the detection information generated is uniformly correlated and fused by the fusion center to form radar fusion track information. At present, distributed processing [23] is widely used in military C3I systems and civil aviation control systems.

The proposed method in this paper is to improve the accuracy of radar target detection based on blockchain under the scenario of multi-source radar fusion processing of the same target detection. A smart contract is a contractual process that is automatically executed based on specific conditions. It is an important way for users to interact with the blockchain and to implement business logic using the blockchain. In this paper, The data

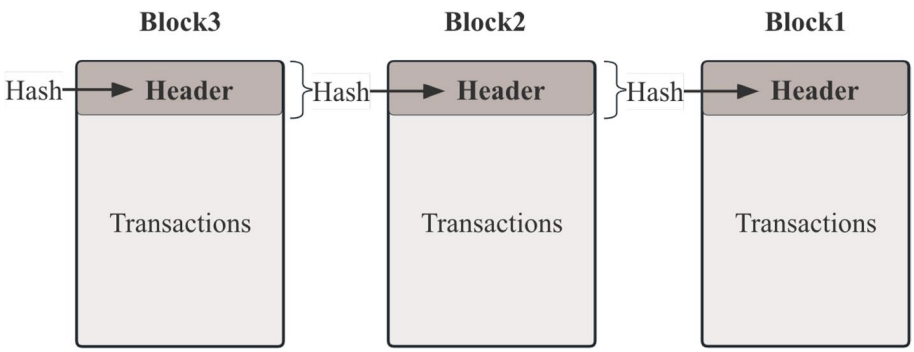

Fig. 3 Block chain structure

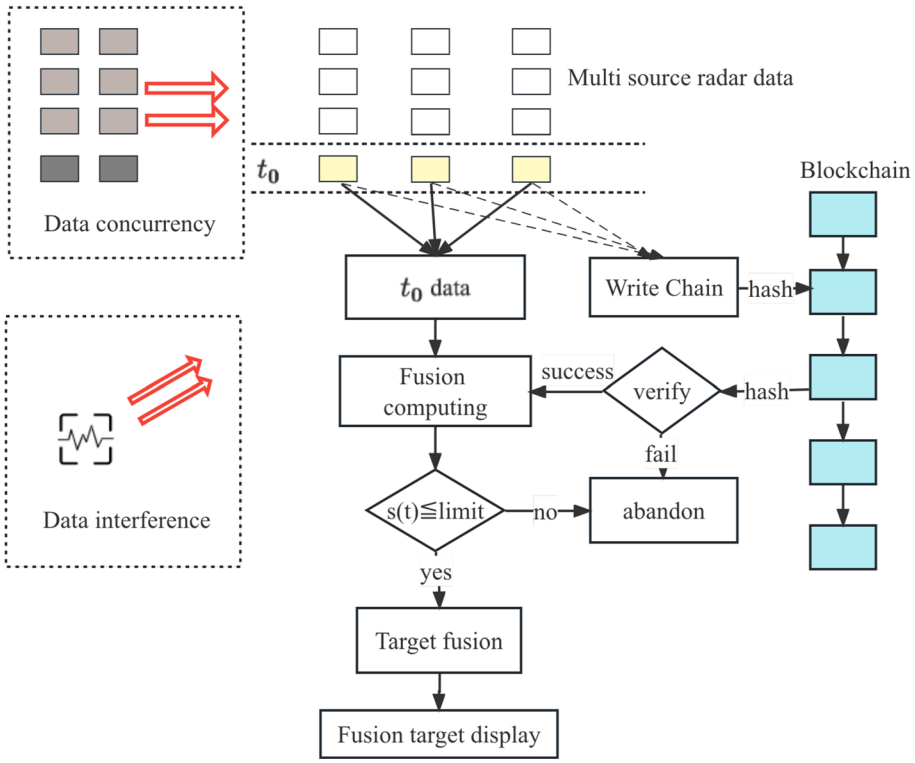

Fig. 4 The Blockchain based data fusion process

fusion process is encapsulated into a smart contract on the chain, which is deployed to the relevant nodes of the blockchain task, resulting in a distributed data validation and processing strategy.

The target position data of the radar [24] comes from the radar echo, which is the position data of the target center point formed after the analog-to-digital conversion and detection of the echo. This position information consists of distance information and angle information between the radar and the target, which is relative position information. The angle information is represented by the angle between the line connecting from the radar to the target and the horizontal line. Therefore, the air target data detected by each radar is a time-based array of radar target positions:

$$V_n = (d_n, \theta_n, v_n, \phi_n), \tag{1}$$

where d is the distance from the radar to the target, θ is the included angle between the line from the radar to the target and the horizontal line, v represents the target velocity detected by the radar, ϕ is the radar azimuth information, n represents the radar serial number and takes the values 1, 2, 3. Assume that three groups of radars detect the same target at the same time, the radar data of each group are V_1, V_2, V_3 in (1). Take target information of three radars at time t_0 for fusion calculation. In this paper, the radar position and range information are selected for fusion calculation and processing, and the target fusion position is obtained through standard deviation calculation and processing. The data processing flow is as follows:

As shown in Fig. 5, the fusion of three selected radar position information d_1, d_2, d_3 in (2) is performed at a certain moment.

$$s = \sqrt{\left(\sum_{i=1}^{n}(d_i - d)^2\right)/n}. \tag{2}$$

This fusion process yields a fused position value, denoted as d. Then, the standard deviation of three radar positions d_1, d_2, d_3, and fusion positions d are calculateed. If the standard deviation s is less than the threshold, the data fusion is considered successful, and the target display is updated. Otherwise, it is considered that the data fusion fails and the data at this moment is discarded. Select the data at each time in turn for the above processing to obtain the final target fusion track. According to

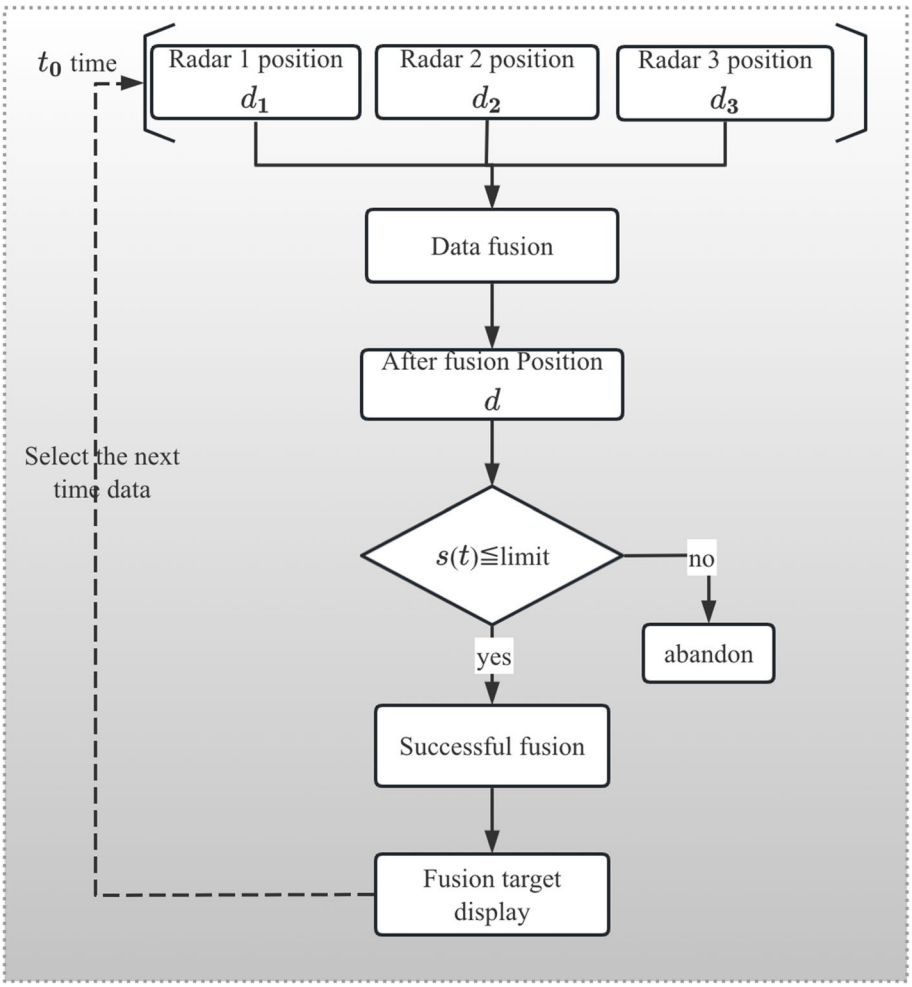

Fig. 5 Data fusion process

the simulation experiment scenario, we set the threshold value to 0.05.

Data closer to the true value track can be formed through data fusion processing. However, if the data of one or more radars are disturbed or destroyed, the fusion success rate will be greatly reduced, and the target fusion result will deviate greatly from the true value track, resulting in a poor fusion effect.

Blockchain has shown its effectiveness in providing strong guarantees for data security and protection. By incorporating blockchain technology, the required data can be securely stored within the blockchain, leveraging its inherent immutability to ensure data security. During the transmission process, data can be safeguarded through hashing and verification processes provided by the blockchain.

In the above multi-source radar data fusion process, before radar distributed processing, the detection data is directly hashed, encrypted, and written into the blockchain from the radar source. Before radar data fusion calculation, the original data is directly obtained from the blockchain, and the security of the data is judged through hash verification. If the data is wrong, it is discarded directly. If the data is valid, it is used as the input of the fusion calculation, and then enters the subsequent data process. Through blockchain processing, the original radar detection data can be ensured to be reliable and safe, and the fusion effect can be effectively improved, so as to improve the accurate acquisition and display of target tracks and further improve the operational decision-making and combat capability. However, the blockchain will bring

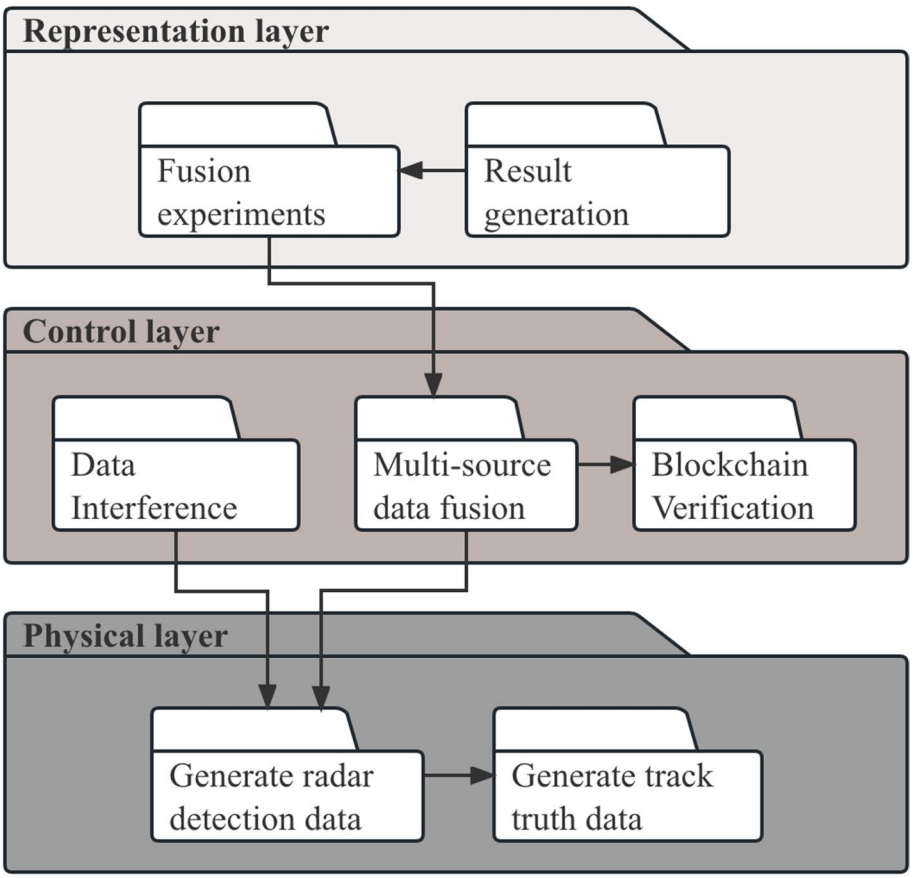

Fig. 6 Simulation system architecture package diagram

additional resource consumption while improving the data performance.

Simulation and results

This section describes the simulation experiments, including the simulation system, experimental condition and experimental settings. And the simulation system subsection mainly describes the system architecture and the sample set of simulation data.

Simulation system

To verify the effectiveness of the technical architecture of this paper, tests under simulation scenarios are done to verify the anti-interference effect of blockchain on data fusion using simulation data.

System architecture

As shown in Fig. 6, the simulation system architecture [25] is divided into 3 layers.

The bottom layer is the data entity layer, including the generation of trajectory true value data package, the generation of radar detection data package. Among them, generating trajectory truth data package is used to generate target trajectory truth data. On the other hand, generating radar detection data package is used to generate detection data generated by 3 groups of radar detection targets, which will have deviation from the truth data.

The middle layer comprises the control layer, which consists of a data jamming package, a multi-source data fusion package, and a blockchain verification package. The data jamming package is used to simulate the jamming of radar detection data, create network attacks, and tamper with data based on specific rules. The multi-source data fusion package is utilized to fuse multi-source data and calculate the fusion result. The blockchain verification package provides data hash uploading, pre-fusion verification, fusion result hash checking, and is introduced to verify the data fusion process by leveraging blockchain technology.

The uppermost layer is the representation layer, which includes the fusion experiment package and the result generation package. These packages are used to conduct simulation experiments and generate simulation results.

Among them, the pseudo-code of the multi-source data fusion algorithm part is shown in Algorithm 1.

Input: t; V_1; V_2; V_3; transactionID; blockchainFlag;
Output: SuccessRate;

```
if blockchainFlag == True then
    calculateOnchainValid(transactionID,V1, V2, V3)
    if result.state == True then
        if result.V1 == True then
            num = num + 1
            V = V + V1
            VSet.append(V1)
        end if
        if result.V2 == True then
            num = num + 1
            V = V + V2
            VSet.append(V2)
        end if
        if result.V3 == True then
            num = num + 1
            V = V + V3
            VSet.append(V3)
        end if
        V = V / num
        n=0
        l=len(set)
        while n < l do
            disSet.append(distance(V,VSet[n]))
            std = stdDis(disSet)
            if std < 0.05 then
                SuccessRate = True
            else
                SuccessRate = False
            end if
            n = n + 1
        end while
        return SuccessRate
    end if
end if
```

Algorithm 1 FuncMulti-sourceDataFusion

Sample set of simulation data

Figure-eight flight refers to the dynamic target navigation in the shape of "eight", which is characterized by diversity, high performance and accuracy. Figure-eight route design is the key step of the figure-eight flight, and the design goal is to allow the dynamic target to accomplish specific tasks such as military, surveillance, and photography. In this paper, a simple figure-eight route is designed using (3).

$$\begin{cases} x = 2cos(3.6t) + 2(3.6t), & t \in [0, 10\Pi]. \\ y = sin(7.2t), & t \in [0, 10\Pi]. \\ z = 0.5, & t \in [0, 10\Pi]. \end{cases} \tag{3}$$

In the experiment of this paper, t is taken from 0 to 10Π evenly divided into 2000 points, each unit moment the target sequence of flight to a point in (3). It is calculated that after every 111 moments, the target will fly around the figure-eight route, the target trajectory true value data is shown Fig. 7.

The manually set parameters in the simulation scenario are shown in Table 1.

The fusion success rate standard deviation threshold is set to 0.05. To simulate a realistic environment, the radar detection data generated for this experiment included more real-value data. In the detection distance attribute, an amplitude error that randomly varied within [-0.05,0.05] km was added. After the measurement, any multi-way radar data fusion that was performed resulted in a fusion point distance standard deviation that was not greater than 0.05. This led to the setting of the fusion success standard deviation threshold at 0.05. During the experiment, the number of interfered data was varied between 0 and 3, which indicated the number of interfered radar detection data sources. The single-way data interference amplitude was taken as [0,1] km, indicating the range of single-way detection data distance information that was interfered with during the experiment. Single-way data jamming success rate indicates the success rate of single-way detection data distance information being interfered with during that experiment, and it was also varied between [0,100], indicating the range of single-way detection data distance information that was interfered with during the experiment. The single-turn flight time is the time it takes for the target to make one turn around the figure-eight route. Among them, the location information of three radars, which are simulated data for simulation experiments. The value range of the number of ways to interfere with data is determined by the number of radars in the simulation experiment. The value range of the fusion success standard deviation threshold and the single-way data interference amplitude is determined by the distance of the radar from the target. The changes in the generation parameters do not have an essential impact on the validation test and do not affect the argument of this thesis.

Experimental condition

In the simulation condition, three radar positions and a target theoretical flight trajectory are shown in Fig. 8. The route is a very important waiting route for aircraft

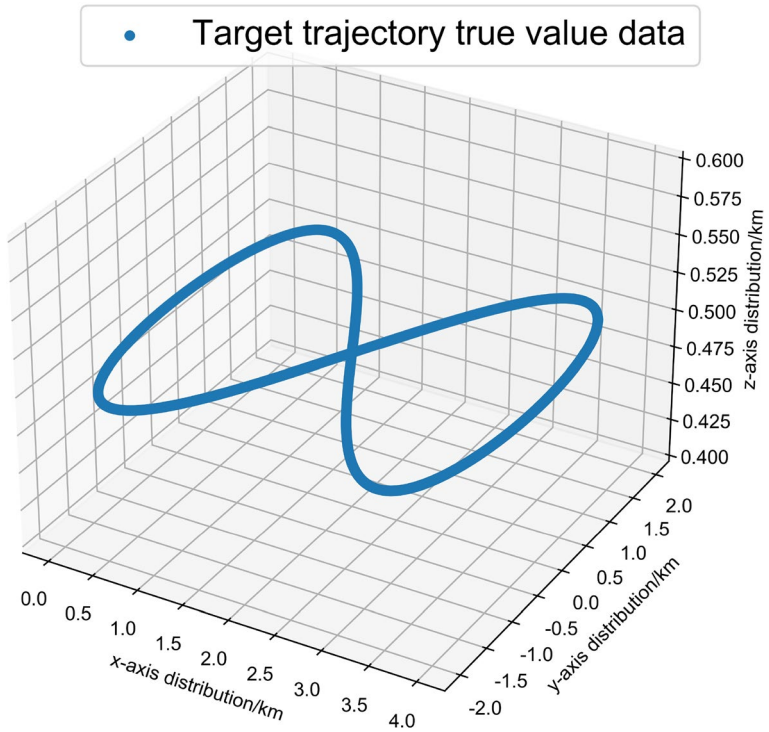

Fig. 7 Target trajectory true value data

Table 1 Parameters 1

Parameters	Value
Radar 1 position coordinates	(2,2,0)
Radar 2 position coordinates	(-2,0,0)
Radar 3 position coordinates	(-2,-2,0)
Fusion success standard deviation threshold	0.05
Number of ways to interfere with data (ways)	[0,3]
Single-way data interference amplitude (km)	[0,1]
Single-way data jamming success rate (%)	[0,100]
Single-turn Flight Time (Single experiment, s)	111

to hover and wait before performing a mission or landing for recovery. There may be multiple aircraft circling and waiting in the route. The accuracy and reliability of detection requirements are high. In the simulation scenario, we consider ship-based [26], shore-based and other types of detection radar, detection of the same target. The data obtained from the multiple radar sources are then fused , and the fused trajectory of the target is obtained.

Experimental settings

Radar jamming [27] is a technology used to disrupt or deceive an enemy's radar equipment by generating electronic interference. It is intended to reduce or eliminate the effectiveness of the radar system. Radar jamming can be classified into two types: suppressive interference and deceptive interference [28]. The former aims to form a strong background of clutter or a large number of false target echoes on the radar display, which reduces the detection ability of the radar. The latter focuses on deceiving the radar operator or the radar automatic tracking system to misidentify the angle, distance, speed, and false target, thus disrupting the identification and tracking of the target.

In the real business scenario, the radar detection data may be interfered in several links. Apart from interference during the radar detection process, radar data is also vulnerable to network attacks [29] after transmission to the server and before the multi-source data fusion stage. These attacks can interfere with or destroy the data stored on the server, reducing the success rate of the data fusion and causing the fused results to deviate from the true values.

Interference damage to the data on the server [30] usually relies on cyber attacks to tamper with the data, such as tampering with radar detection distance information, azimuth information, pitch angle information, or tampering with radar detection data moments. When the data is tampered with, the data source used for multi-source data fusion is damaged, and the fusion success rate is greatly reduced and the fusion effect becomes poor.

The above interference can be categorized into two types, data tampering [31] type and chaotic sequence

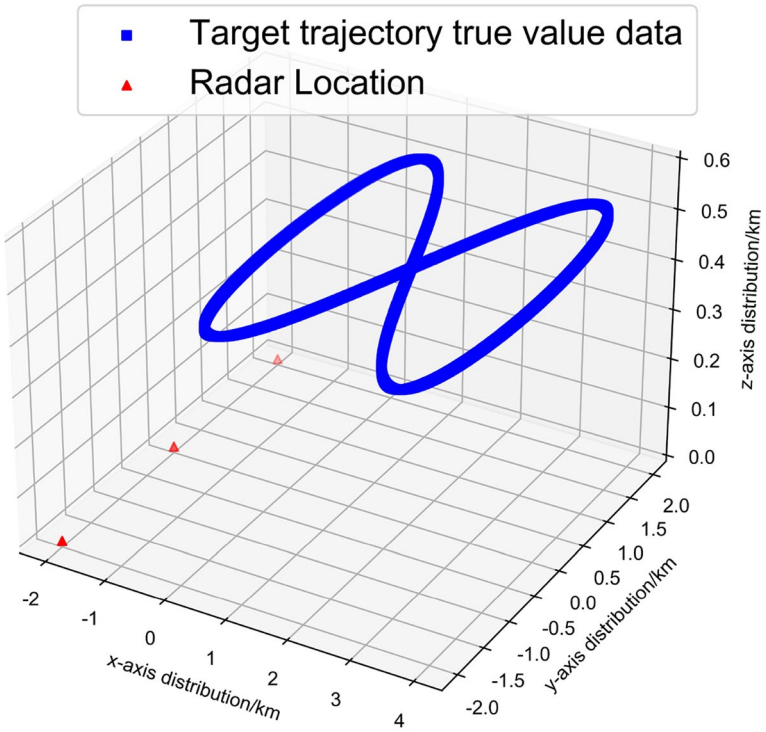

Fig. 8 Simulation scene

tampering [32] type. There are two types of interference related to data tampering. The first type involves tampering with and damaging any one or more data categories, including radar detection distance information, azimuth information, and pitch angle information. The second type is chaotic sequence tampering, which involves tampering with and damaging the radar detection timing. The above types of interference can be described by the characteristic values of the dimensions of interference success probability, interference magnitude, and number of interference paths.

In this experiment, we design the interference as follows.

First, we fix the interference path number eigenvalue as 3, fix the interference amplitude, change the single-way data interference success rate, and calculate the relationship between the fusion success rate and the interference success rate under different interference success rates. Second, we fix the interference path eigenvalue as 3, fix the single data interference success rate, change the interference amplitude, and calculate the fusion success rate versus interference amplitude for different interference amplitudes.

This experiment aims to compare two groups: one without interference and one with interference. Within the group with interference, two categories of interference will be considered, namely interference amplitude and interference success rate. For each category, a comparison will be made between the results obtained without blockchain implementation and those obtained with blockchain implementation. The effectiveness of blockchain on the characteristic dimensions of interference amplitude and interference success rate is verified respectively.

A: Interference-free situation

In the case of no interference, the data detected by the three groups of radar are fused to obtain the multi-source fusion data and the fusion success rate.

B: With interference case, interference amplitude variation for each data channel

1) Interference success rate fixed 50%, interference amplitude variation for each data path, no block chain

Fusion of 3 sets of radar-detected data in the presence of interference to obtain multi-source data fusion success rate.

2) Interference success rate fixed 50%, interference amplitude variation for each data path, blockchain implemented

In the presence of interference, the data from 3 groups of radar detections are fused, and the data from each path is verified on the chain to get the multi-source data fusion success rate.

C: In the presence of interference, the interference success rate of each road data changes

1) Interference amplitude fixed 1km, per-way data interference amplitude change, no block chain

fusion of 3 sets of radar-detected data in the presence of interference to obtain the multi-source data fusion success rate.

2) Interference amplitude fixed 1km, per-way data interference success rate variation, blockchain implemented

In the case of interference, the data detected by 3 groups of radar are fused, and the data of each path is verified on the chain to get the multi-source data fusion success rate.

D: With interference case, multi-source fusion processing efficiency per unit time

1) Interference amplitude fixed 1km, per-way data interference amplitude change, no block chain

The fusion of data detected by 3 groups of radar in the presence of interference to obtain the multi-source fusion data processing efficiency.

2) Interference amplitude fixed 1km, per-way data interference success rate variation with block chain

fusion of data from 3 sets of radar detections in the presence of interference, with each data up-chain validation, to obtain the multi-source fusion data processing efficiency.

Numerical results

This section presents the experimental numerical results from the execution of the comparison tests described in Section "Simulation and results".

A: No interference situation

As shown in Fig. 9, the fused radar detection trajectory close to the true value data is obtained in the absence of interference.

The success rate of multi-source data fusion is 100% in the absence of interference.

B: With interference, each data interference amplitude change

The manually set parameters in the simulation scenario are shown in Table 2.

As shown in the Fig. 10, blockchain implemented validation, the fusion success rate is higher than non-blockchain implemented validation when the per-way data interference magnitude is greater than 0.2km. The larger the per-route data interference amplitude is, the impact on the fusion success rate tends to be stable with or non-blockchain implemented verification.

In the presence of a blockchain, if data from a particular source is tampered with, the data will fail to pass the uplink verification, and as a result, it will not be used in the fusion process. Instead, the other available data sources are fused to improve the fusion success rate. Regarding the input parameters, the success rate of

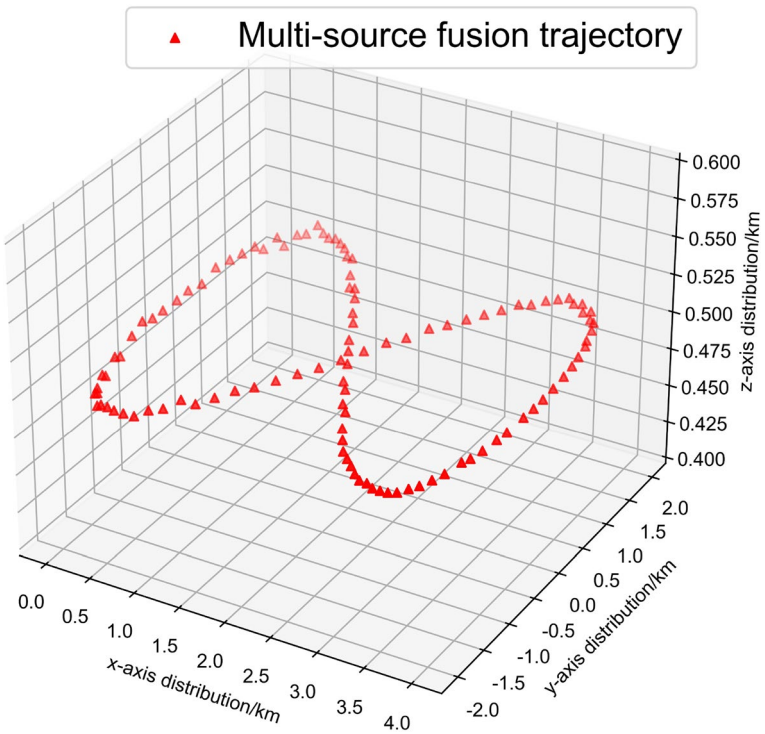

Fig. 9 Interference-free fusion trajectory

Table 2 Parameters 2

Parameters	Value
Radar 1 position coordinates	(-2,2,0)
Radar 2 position coordinates	(-2,0,0)
Radar 3 position coordinates	(-2,-2,0)
Fusion success standard deviation threshold	0.05
Number of ways to interfere with data (ways)	3
Single-way data interference amplitude (km)	[0,1]
Single-way data jamming success rate (%)	50
Single-turn Flight Time (Single experiment, s)	111
Number of tests	100

interference for each data source is set to 0.5. When all three data sources are interfered with at the same time, the data at that time will not pass the uplink verification, and there will be no untampered data available for fusion. As a result, there may be cases of fusion failure.

C: With interference case, the change of interference success rate for each data path

The manually set parameters in the simulation scenario are shown in Table 3.

As shown in Fig. 11, blockchain implemented verification, the fusion success rate is higher than non-blockchain implemented verification when the success rate of data interference is less than 100% for each path. When the data interference success rate is at 100%, the impact on the fusion success rate is basically the same with or non-blockchain implemented verification.

Based on the input parameter, the interference amplitude for each data source is set to 1 km. When all three data sources are interfered with at the same time, the data at that time will not pass the uplink verification, and there will be no untampered data sources for fusion. Therefore, there may be instances of fusion failure. When the success rate of interference for each data source is low, even if one of the data sources is not interfered with, the blockchain can still exhibit a significant anti-interference effect. However, when the success rate of interference for each data source is high, there is a greater chance that all three data sources will be interfered with simultaneously, which can weaken the anti-interference effect of the blockchain.

We have done experiments on the impact of parameter changes in both dimensions on the fusion success rate, and the simultaneous changes of parameters in both dimensions affect the fusion success rate, but in general, both have a positive impact on the data fusion success rate.

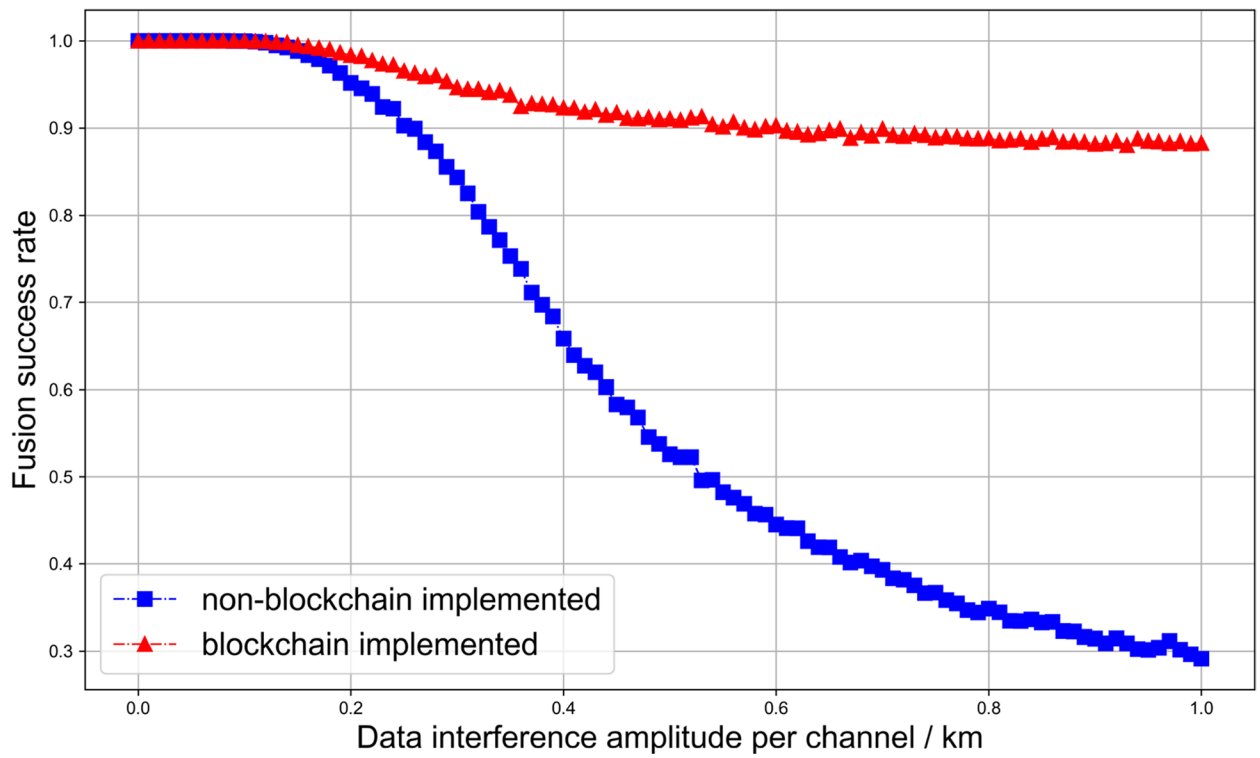

Fig. 10 Fusion success rate versus single-way data interference amplitude

Table 3 Parameters 3

Parameters	Value
Radar 1 position coordinates	(-2,2,0)
Radar 2 position coordinates	(-2,0,0)
Radar 3 position coordinates	(-2,-2,0)
Fusion success standard deviation threshold	0.05
Number of ways to interfere with data (ways)	3
Single-way data interference amplitude (km)	1
Single-way data jamming success rate (%)	[0,100]
Single-turn Flight Time (Single experiment, s)	111
Number of tests	100

D: With interference, multi-source fusion processing efficiency per unit time

According to Fig. 12, which shows the processing elapsed time statistics for the experiments in 5.D, we can obtain the fusion elapsed time for a single experiment consisting of 111 sets of points.

The average elapsed time is 0.0003873475707403504ms/111 points for the non-blockchain implemented approach and 0.0015085050375154704ms/111 points for the blockchain-implemented approach. Based on these results, we can calculate the fusion processing efficiency to be 286564338 transactions per second (tps) for the blockchain-implemented approach and 73582784 tps for the non-blockchain implemented approach.

Among the experiments that blockchain implemented, 36 experiments took more than 50ms, accounting for about 0.356% of the total number of experiments. When the blockchain reads and writes are conducted within the same block, the retrieval time is reduced and less time-consuming. On the other hand, when the reading and writing to the blockchain occur during the outgoing block interval, it increases the retrieval time, which can impact the fusion time for the current experiment. When both blockchain reads and writes are performed within the same block, the retrieval time is lower and less time-consuming. However, if the reads and writes occur in different blocks, the retrieval time increases, which can affect the overall fusion time of the experiment. However, the overall fusion time is still relatively small and will not have a large impact for a normal detection task.

As shown in Table 4, after adding blockchain validation, the fusion processing efficiency is lower than the case non-blockchain implemented validation, with 74.85% lower processing efficiency. The reasons for the reduced efficiency of fusion processing are the following.

1) Data up-chaining consumption. For each moment of the fusion process, there are two uploads: the first for the data original information hash upload, and the second

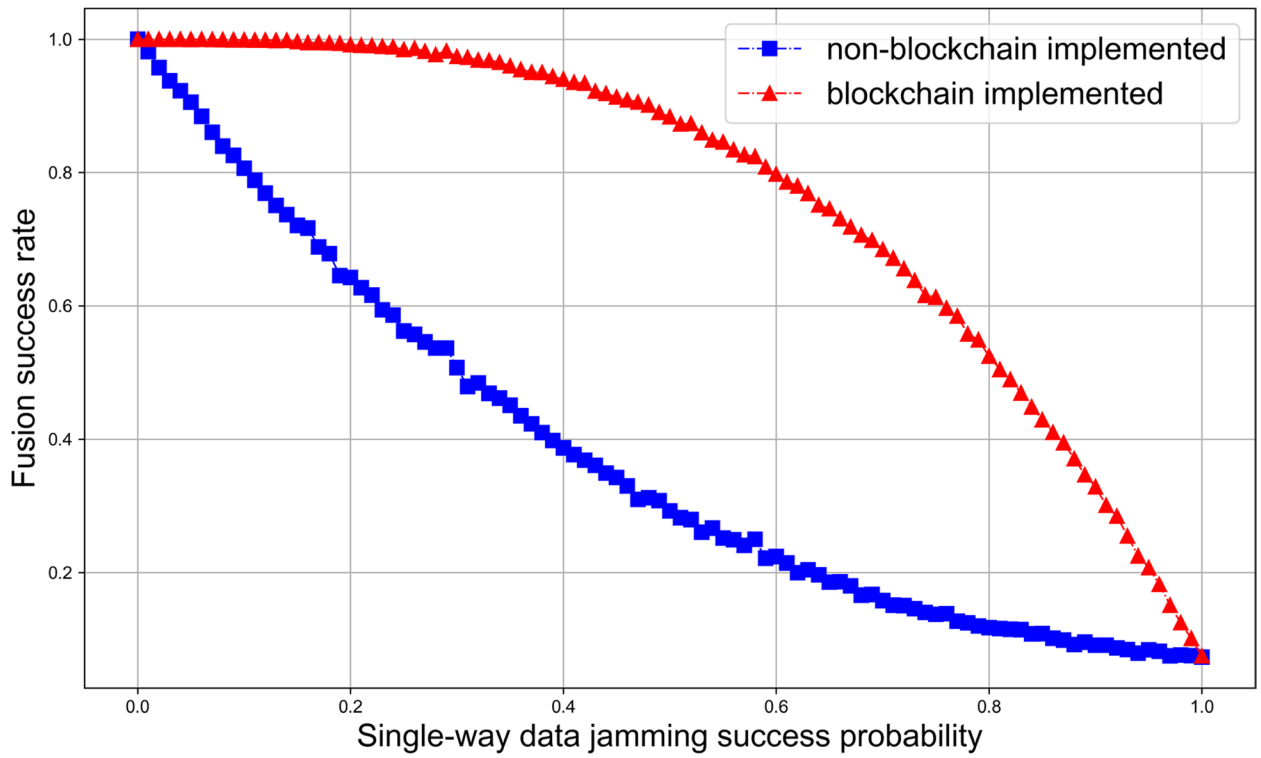

Fig. 11 Relationship between fusion success rate and per-way data interference success probability

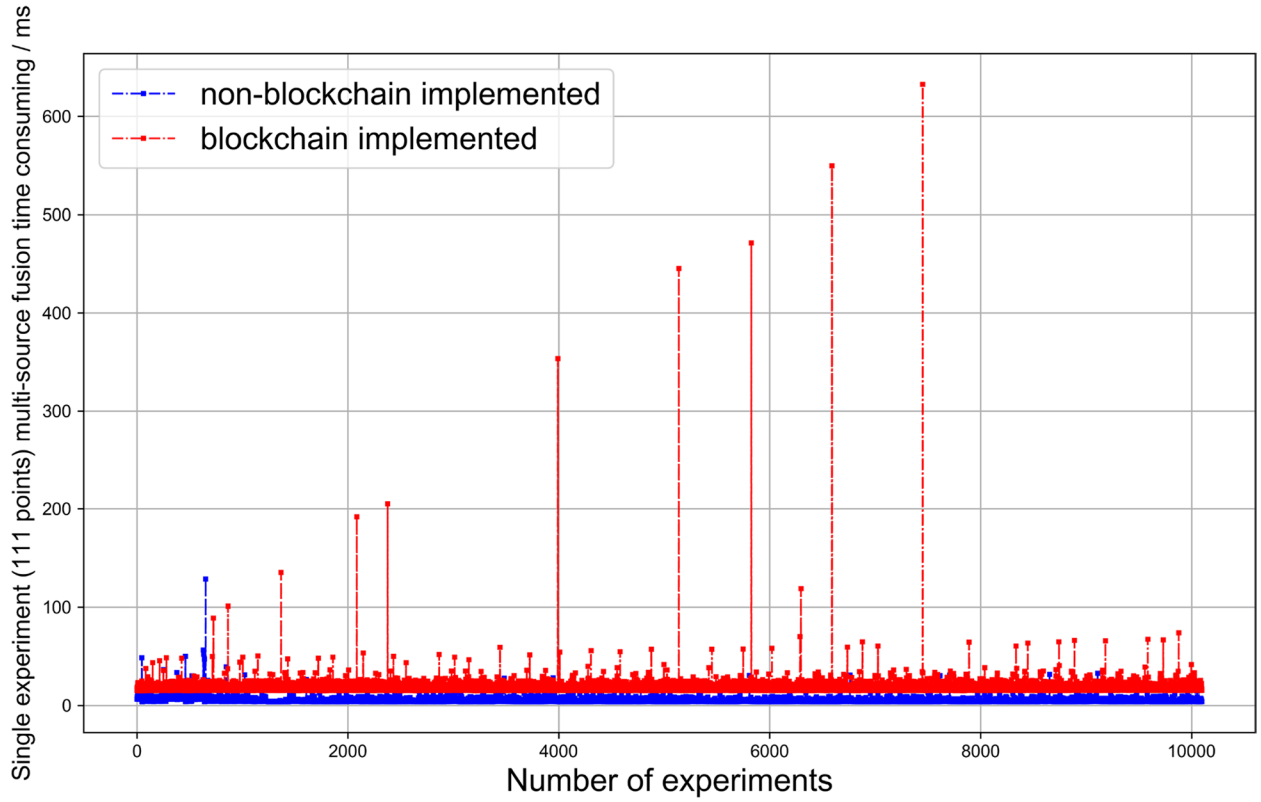

Fig. 12 Single experiment (111 points) multi-source fusion time consuming

Table 4 Fusion processing efficiency

	non-blockchain implemented	blockchain implemented
Fusion processing efficiency (tps)	286564338	73582784

for the fusion result to be hashed upload. Through controlled experimental analysis (shown in Table 5), the two data uploads consume about 49.13% and 7.67% of the efficiency reduction, respectively.

2) Data reliability retrieval consumption. Before fusion, the data to be fused need to be verified once on the blockchain to get the verification results, and the reliability retrieval consumption accounts for about 41.04% of the efficiency reduction through the analysis of the controlled experiment.

3) Complex interaction logic consumption. Before and after the fusion, the complexity of the system is increased, and the consumption of complex interaction logic accounts for about 2.16% of the efficiency reduction through the analysis of controlled experiments.

Conclusion

This paper proposes a new architecture for a trusted execution environment with integrated blockchain capability in the context of multi-source data fusion. To evaluate the effectiveness of this architecture, a simulation experimental system for generating radar detection and target trajectory data is built and a

Table 5 Time consuming

	non-blockchain implemented	blockchain implemented
Control group (ms)	0.0003873475707403504	0.0015085050375154704
Removal of the fusion result winding process (ms)	0.0003795104451698832	0.001435657538989983
Removal of blockchain verification, fusion results on the chain process (ms)	0.0003726647631956799	0.0009594105257846341
Removing the process of data source uplinking, blockchain validation, and fusion results uplinking (ms)	0.00038555352994711095	0.0004102924082538869

jamming environment for tampering and corrupting the data is simulated. This paper then uses pair group comparison experiments to verify the effectiveness of blockchain in building a trusted execution environment and improving the success rate of multi-source target fusion. Experimental results suggest that blockchain can effectively prevent data tampering and enhance the fusion effect in the system of multi-source data fusion scenario. Moreover, blockchain can improve the fusion success rate by more than 50% when the magnitude of data interference is large, and the maximum fusion success rate can be improved by more than 50% when the success rate of multiplex interference changes. Although blockchain brings a limited performance load with a 74.85% performance drop, it can still support the normal operation of business scenarios. Finally, it is noted that blockchain inheritance shows a high comprehensive operational effectiveness.

Future work

This paper describes the application of blockchain for improving the accuracy of multi-source data fusion in the scenario of multi-source radar for multi-source data fusion processing for the same target detection. The experimental data shows that the blockchain technology is effective in solving the problem of distributed data sharing security. However, such security measures consume data on the chain, which results in a reduction of fusion efficiency. Therefore, it is necessary to find a balance between multi-source data fusion data security and data processing performance.

In this paper, researchers have performed performance modeling and analysis of the block propagation protocol to address the impact of key blockchain parameters on overall performance. One optional approach involves using hardware encryption to enhance signature verification performance. Furthermore, reducing decentralization by introducing consensus agreements has also been proposed as a means for improving blockchain performance.

Authors' contributions

Nan Yang, Li Yang and Xingzhou Du wrote the main manuscript text, Nan Yang and Xingzhou Du did the experimental verification, Li Yang and Xunyi Guo prepared the pictures, Yuwen Zhang and Fanke Meng were involved in the study of some specific technical points and the discussion of experimental steps, and all the authors reviewed and revised the manuscript.

Funding

None.

Availability of data and materials

Data were obtained from a simulation modeling environment.

Declarations

Ethics approval and consent to participate

Not applicable.

Competing interests

The authors declare no competing interests.

Received: 31 March 2023 Accepted: 28 July 2023
Published online: 19 August 2023

References

1. Wang Y, Chen L (2017) Multi-view fuzzy clustering with minimax optimization for effective clustering of data from multiple sources. Expert Syst Appl 72:457–466. https://doi.org/10.1016/j.eswa.2016.10.006
2. Chen Cs, Hu Hr, Fang Ll, Xiang Yx (2020) Research on equipment situation display based on multi-source data fusion. In: 2020 International Conference on Computer Engineering and Intelligent Control (ICCEIC), pp 207–211. https://doi.org/10.1109/ICCEIC51584.2020.00048
3. Li D, Zhang J, Xu R, Meng J, Wang J, Chen X et al (2022) A multisource data fusion modeling prediction method for operation environment of high-speed train. Discret Dyn Nat Soc 2022:1–9
4. Geng G, Xiao Q, Liu S, Liu X, Cheng J, Zheng Y et al (2021) Tracking air pollution in China: near real-time pm2.5 retrievals from multisource data fusion. Environ Sci Technol 55:12106–12115
5. Fu Y, Yu FR, Li C, Luan TH, Zhang Y (2020) Vehicular blockchain-based collective learning for connected and autonomous vehicles. IEEE Wirel Commun 27(2):197–203. https://doi.org/10.1109/MNET.001.1900310
6. He B, Su H, Huang J (2021) Joint beamforming and power allocation between a multistatic mimo radar network and multiple targets using game theoretic analysis. Digit Signal Process 115(5):103085
7. Zhang G, Tian G, Cai D, Bai R, Tong J (2021) Merging radar and rain gauge data by using spatial-temporal local weighted linear regression kriging for quantitative precipitation estimation. J Hydrol 601(1):126612
8. Chen P, Zheng L, Wang X, Li H, Wu L (2017) Moving target detection using colocated mimo radar on multiple distributed moving platforms. IEEE Trans Signal Process 65(17):4670–4683. https://doi.org/10.1109/TSP.2017.2714999
9. Jia J, Zhao Q, Xu Z, Meng D, Leung Y (2021) Variational bayes' method for functions with applications to some inverse problems. SIAM J Sci Comput 43(1):355–383. https://doi.org/10.1137/19M130409X
10. Liu Q, Zhang H (2022) Reliability evaluation of weighted voting system based on d-s evidence theory. Reliab Eng Syst Saf 217:108079
11. Zhou K, Tang J (2021) Efficient characterization of dynamic response variation using multi-fidelity data fusion through composite neural network - ScienceDirect. Eng Struct 232. https://doi.org/10.1016/j.engstruct.2021.111878
12. Hasan MK, Alkhalifah A, Islam S, Babiker NBM (2022) Hossain MA (2022) Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations. Wirel Commun Mob Comput 9:1–26
13. Li C, Fu Y, Yu FR, Luan TH, Zhang Y (2020) Vehicle position correction: A vehicular blockchain networks-based gps error sharing framework. IEEE Trans Intell Transp Syst PP(99):1–15
14. Gourisetti SNG, Sebastian-Cardenas DJ, Bhattarai B, Wang P, Widergren S, Borkum M, Randall A (2021) Blockchain smart contract reference framework and program logic architecture for transactive energy systems. Appl Energy 304:117860
15. Du J, Chen H, Yan G, Niu Z, Shi Z, Hu Y (2022) Research on the application of blockchain technology in the weapon and equipment testing. In: 2022 International Conference on Computer Network, Electronic and Automation (ICCNEA), pp 234–237. https://doi.org/10.1109/ICCNEA57056.2022.00059
16. Hsiao SJ, Sung WT (2023) Enhancing cybersecurity using blockchain technology based on IoT data fusion. IEEE Internet Things J 10(1):486–498. https://doi.org/10.1109/JIOT.2022.3199735

17. Yang J, Wen J, Jiang B, Wang H (2020) Blockchain-based sharing and tamper-proof framework of big data networking. IEEE Netw 34(4):62–67
18. Kumar A, Fischer C, Tople S, Saxena P (2017) A traceability analysis of monero's blockchain. https://doi.org/10.1007/978-3-319-66399-9_9
19. Wang Y, Li J, Zhao S, Yu F (2020) Hybridchain: A novel architecture for confidentiality-preserving and performant permissioned blockchain using trusted execution environment. IEEE Access 8:190652–190662
20. Distler T (2021) Byzantine fault-tolerant state-machine replication from a systems perspective. ACM Computing Surveys (CSUR)
21. Silva CA, Duncanson L, Hancock S, Neuenschwander A, Dubayah R (2021) Fusing simulated gedi, icesat-2 and nisar data for regional aboveground biomass mapping. Remote Sens Environ 253(112):234
22. Guillem R, García S, Madrigal J, Barrera D, Gasulla I (2018) Few-mode fiber true time delay lines for distributed radiofrequency signal processing. Opt Express 26(20):25761
23. Du L, Sun Q, Bai J, Wang J (2021) A verification method for traffic radar-based speed meter with target position determination in road vehicle speeding enforcement. IEEE Trans Veh Technol 70(12):12374–12388. https://doi.org/10.1109/TVT.2021.3116110
24. Lickleder T, Hamacher T, Peri VS (2021) Thermohydraulic model of smart thermal grids with bidirectional power flow between prosumers. Energy 230. https://doi.org/10.1016/j.energy.2021.120825
25. Fu Y, Li C, Yu FR, Luan TH, Zhang Y (2020) An autonomous lane-changing system with knowledge accumulation and transfer assisted by vehicular blockchain. IEEE Internet Things J PP(99):1
26. Xiong Y, Yu J, Tu Y, Pan L, Mou J (2021) Research on data driven adaptive berthing method and technology. Ocean Eng 222(24):108620
27. Lan L, Liao G, Xu J, Zhang Y, Zhu S (2020) Mainlobe deceptive jammer suppression using element-pulse coding with mimo radar. Signal Process 182(May (5)):107955
28. Li Y, Gao Z, Huang L, Du X, Guizani M (2018) Energy-aware interference management for ultra-dense multi-tier hetnets: Architecture and technologies. Comput Commun 127(sep.):30–35
29. An H, Na Y, Lee H, Perrig A (2021) Resilience evaluation of multi-path routing against network attacks and failures. Electronics 10(11):1240
30. Hu J, Moorthy SK, Harindranath A, Zhang Z, Zhao Z, Mastronarde N, Bentley ES, Pudlewski S, Guan Z (2023) A mobility-resilient spectrum sharing framework for operating wireless uavs in the 6 ghz band. IEEE/ACM Trans Networking 1–15. https://doi.org/10.1109/TNET.2023.3274354
31. Guo J, Wang X, Xue W, Zhao Y (2021) System identification with binary-valued observations under data tampering attacks. IEEE Trans Autom Control 66(8):3825–3832. https://doi.org/10.1109/TAC.2020.3029325
32. Yu W, Wang H (2021) Analysis of trigonometric chaotic sequence by proposing an index-based bit level scrambling image encryption. Mod Phys Lett B. https://doi.org/10.1142/S0217984921504066

Publisher's Note