Image Processing, Electronics and Computers
L. Trajkovic et al. (Eds.)

doi:10.3233/ATDE240506

Research on Communication Network Security of Unmanned Surface Vehicle Based on Block Chain

Shan JIANG[1] and Hengbo ZHANG
No.92493 troops of PLA, Huludao, China

Abstract. The communication network security of unmanned surface vehicle (USV) is the central problem to ensure the stable operation and data transmission of boat system. Based on block chain, this paper studies the communication network security of USV. By introducing the block chain technology into the communication network of USV, the design of identity authentication mechanism based on block chain was made, and the protection method of data integrity was proposed. Then the decentralized trust model is made to provide the protection in aspects of identity authentication, data integrity, non-repudiation and network defense. To verify the feasibility and effectiveness of the security mechanism, the construction of simulation environment was built and the experiments were done, which was built for the communication network of USV based on block chain. The paper shown that the application of block chain in the cyber security of USV was worthy of study.

Keywords. USV, communication network, block chain, network defense

1. Introduction

With the increasingly fierce competition in the ocean, unmanned surfacewater vehicle (USV) will play a greater role as a new maritime combat platform, and its research work has been rapidly developed [1-2]. Due to the wide range of application scenarios and intense confrontation, the networks of USVs face increasing threats and risks [3-5]. Xun Peng et al. [6] proposed a new paradigm of edge cloud collaboration to solve the problems of poor timeliness and large resource consumption in USV. Agogino et al. [7] proposed an evolutionary algorithm to solve the communication problem of unmanned networks, which is communicating with ground users through a single broad-spectrum communication channel. Sachan et al. [8] proposed a secure routing protocol based on hash function authentication, which can effectively prevent black holes, modify routing information and simulate attacks. However, there are few researches on wireless communication security of USV based on blockchain technology.

The block chain is a decentralized distributed ledger technology that is characterized as secure, transparent, immutable, and highly trusted [9-11]. The application of block chain in the communication networks security of USV can increase security, protect privacy and prevent unauthorized access. The purpose of this paper is to propose a new security mechanism based on block chain to strengthen the

[1] Corresponding Author: Shan Jiang, 147376173@qq.com

communication network security of USV. By introducing the block chain's features such as consensus mechanism, distributed storage and smart contracts, a secure communication network will be established to protect the communication network OF USV from malicious attacks and data leaks. An experiment was done and the results shown that the security mechanism based on block chain is highly effective in protecting data integrity, providing identity authentication, realizing non-repudiation and enhancing network defense.

2. Related Work

This section will review some important work and methods.

2.1. Security Guarantee Methods

Security methods include access control, encryption, authentication and firewall. However, these traditional methods of security have some limitations [12] in communication network of USV. For example, the RBAC model is difficult to solve the problem of decentralized trust, while communication network of USV often faced special requirements such as wide distribution of nodes and peer-to-peer communication. Traditional encryption and authentication methods may not be able to meet the transmission and verification requirements [13] of massive data in the USV. Border defense devices such as firewalls also cannot completely prevent malicious acts and attacks from within network.

2.2. The Application of Block Chain in the USV.

Because of its decentralized, distributed, immutable and highly trusted characteristics, block chain has attracted wide attention from academia and industry. In recent years, researchers have begun to explore the application of block chain in the cyber security of USV to address the limitations of traditional security assurance methods [14].

In communication network of USV, block chain can be applied in aspects such as identity authentication, data integrity protection, non-repudiation assurance and network defense. Utilizing the distributed storage and smart contract functions of block chain can ensure the integrity and reliability of the data transmitted in the communication network of USV [15]. The immutability and smart contracts of block chain can provide non-repudiation guarantees against tampering and denial of operations. In addition, the block chain's functions such as consensus algorithm and distributed storage can be used to build a powerful network defense mechanism and enhance the anti-attack capability of the USV.

2.3. Existing Challenges

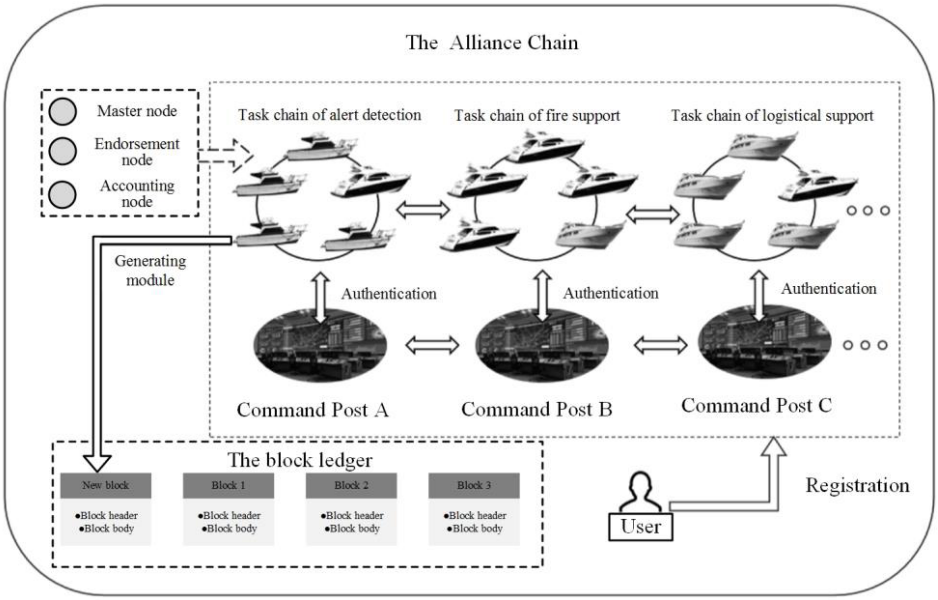

Figure 1. The mission architecture of the USV formation based on block chain

While block chain has potential in the cyber security of USV, there are still some challenges. Future research directions include but are not limited to the following aspects: First, research on how to integrate traditional security methods and block chain in the communication network of USV to provide more comprehensive and robust security. Secondly, the performance optimization and scalability of block chain need to study in depth to adapt to the real-time and bandwidth requirements of the USV's communication network. In addition, research on how to establish a suitable privacy protection mechanism in the USV to protect the security of user data and privacy [16,17].

Block chain has a wide range of application in the cyber security of USV. Through further research and improvement, block chain was applied to the communication network of USV and the task chain architecture is built as shown in Figure 1, which can effectively solve the limitations of traditional security methods, provide a more secure and trusted communication environment, and promote the development of unmanned boat technology[18].

3. Design of Identity Authentication Mechanism Based on Block Chain

The identity authentication based on block chain is an important application of block chain technology in the USV, which realizes decentralized identity authentication and trusted authorization by utilizing distributed ledger and smart contract. In the identity authentication mechanism based block chain, the techniques are used as follow.

(1) Digital signature: The formula of the user's digital signature can be expressed as Sig = sign (SK, Data).

(2) Smart contract: By writing smart contract code, defining verification rules and processes, identity information storage and verification functions are realized. Smart

contract has the ability to execute code, which can verify the identity information provided by the user automatically.

(3) The consensus algorithm of block chain: The consensus algorithm is based on complex mathematical calculations to ensure the security of the distributed ledger.

The identity authentication mechanism based on block chain can be implemented by the following algorithms, which include steps such as registering identity information, authentication requests and authentication process:

(1) Register identity information

Enter: User identification information (ID) and related authentication credentials (Credential).

Process: Generate the user's public key (PK) and private key (SK), and register the user's identity information and PK into the distributed ledger of the block chain.

(2) Authentication requests

Input: User identification information and digital Signature.

Output: Verification request.

Procedure: Use the user's private key to digitally sign the signed Data, and obtain Signature = sign (SK, Data). Construct verification request: Verification_Request = {User ID, Signature}.

(3) The authentication process

Enter: Verification_Request.

Output: Verification_Result.

Process: Get the user's public key information (PK) and identity information (ID) from the block chain. Using public key (PK) to verify the digital signature of the request and determine its completeness and correctness. If the digital signature verification passes, the verification request is valid and further identity information verification is carried out. Use identity information (ID) and other relevant authentication credentials for verification to ensure that the user's identity information is legitimate and valid. If the authentication is successful, the verification result is returned: Verification_Result = {UserID, Verification_Status}.

4. Data Integrity Protection Method Design

The data integrity protection mechanism based on block chain aims to ensure the integrity and reliability of the data transmitted in the USV by utilizing the distributed ledger and smart contract functions of the block chain. This mechanism protects the integrity of data based on the following steps:

(1) Data hash generation: Get the data to be transferred (Data); Use the hash algorithm (SHA-256) to generate a hash value for the data, expressed as Hash Value.

(2) Data upload to the block chain: the verification node packages the data hash value and related verification information (such as time stamp, data source, etc.) and uploads it to the block chain. Use smart contracts to write data hashes and other information into the distributed ledger of the block chain.

(3) Data verification process: the receiving node obtains the hash value of the data and related verification information from the block chain. Hash the received data to generate a new hash value. The generated new hash value is compared with the hash value in the block chain to verify the integrity of the data.

The pseudo-code of the algorithm is as follows.

Algorithm: Identity authentication mechanism based on block chain

```
# Data transfer party
Input: Data
Output: HashValue
# step 1: Data hash generation
HashValue = hash(Data)
# step 2: The data is uploaded to the block chain
UploadToBlockchain(HashValue)
# data receiver
Input: HashValue
Output: Verification_Result
# step 3: Data validation process
NewHashValue = hash(Data)
if NewHashValue == HashValue:
    Verification_Result = "Data integrity verified"
else
    Verification_Result = "Data integrity compromised"
```

5. Design of Non-repudiation Guarantee Scheme Based on Block Chain

Algorithm: Non-repudiation guarantee

```
# Submission of a transaction or operation
Submit (Transaction)
# Verification of Smart contract
def SmartContract (Transaction)
  if Validation_Rules (Transaction) == True
    Verification_Result = "Valid"
  else
    Verification_Result = "Invalid"
  return Verification_Result
# Execution of the transaction or operation
if  SmartContract (Transaction) == "Valid"
  Execute(Transaction)
# Non-repudiation protection
def Non-Repudiation_Guarantee(Transaction):
  Transaction_Hash = hash(Transaction)
  Transaction_Record = Blockchain.query(Transaction_Hash)
# Query the transaction record in the block chain
  if  Transaction_Record != None
    Verification_Result = "Valid - Non-Repudiated"
  else
    Verification_Result = "Invalid - Repudiated"
    return Verification_Result
```

The non-repudiation guarantee mechanism based on block chain aims at the transactions and operations in the USV, and ensures its non-repudiation by utilizing the immutability of block chain and the function of smart contracts.

(1) Submit a transaction or operation: The user submits a transaction or operation request through the communication network of the USV and sends it to the block chain.

(2) Smart contract verification: In the block chain, smart contracts are responsible for verifying the legality and validity of submitted transactions or operations. Smart contracts use pre-set rules and logic to verify transactions or operations and generate corresponding verification results.

(3) Execution of the transaction or operation: Once the transaction or operation has passed the verification of the smart contract, it will be executed and written into the

distributed ledger of the block chain. The execution process is carried out through the automatic execution function of the smart contract.

(4) Non-repudiation guarantee: important information such as execution results and time stamps of transactions or operations are recorded in the block chain, which can be used as evidence of non-repudiation. The immutability of block chain guarantees the accuracy and immutability of the results of transactions or operations, making them non-repudiable.

This mechanism ensures the non-repudiation of transactions or operations in the USV through the automatic execution of smart contracts and the immutable nature of the block chain. By providing the verification results of transactions or operations and records on the block chain, it can provide undeniable evidence and avoid the denial of transactions and the denial of operations.

6. Simulation Verification and Analysis

6.1. Construction of Simulation Environment

This section established a simulation environment based on block chain to make the experiment about identity authentication, including USVs, communication equipment and block chain nodes. Use simulation software and programming language (such as Python) to create the simulation environment to simulate the communication process by setting the relevant parameters. Design an authentication mechanism based on block chain, including steps such as identity information generation, authentication requests, verification of block chain nodes and return of verification results. The simulation about the communication between USVs and block chain nodes was made and different authentication scenarios were set up, such as new user registration, authentication updates, etc. The performance of block chain authentication mechanisms was evaluated by analyzing the data such as communication time, verification result, verification accuracy and verification time in each authentication experiment.

6.2. The Verification of Authentication Scheme

The following steps are taken to authenticate the communication network identity of USV.

Identity information generation: Each USV generates unique identity information, such as public and private key pairs, before joining the communication network.

Registration process: The USV registers its identity information on nodes the of block chain. When registering, it sends a registration request (containing identity information) to the block chain node.

Verification by block chain node: After receiving the registration request, the block chain node verifies the identity information of the USV. The verification process includes verifying the uniqueness, legality and validity of the identity information.

Verification result return: The block chain node returns the verification result (pass or fail) to the USV.

The experiment was done about identity authentication scheme based on block chain in simulation environment, assuming that 100 USVs join the communication network and the average communication time is 2.5 seconds. Among the 100 identity authentication experiments, 98 unmanned boats passed the authentication, the

verification accuracy reached 98%, and the average verification time was 1.5 seconds. The specific data are shown in Table 1.

Table 1. The results of the experiment about identity authentication scheme

Methods	Communication time (seconds)	Verify accuracy (%)	Verification time (seconds)
Blockchain-based	2.5	98	1.5
Traditional	4	92	2
Token-based	3	95	1.8
Certificate-based	3.5	97	2.2

6.3. Verification of Data Integrity Protection Scheme

In the communication network of USV, the integrity of the data needs to be protected to prevent the data from being tampered with or damaged.

Data generation: In a simulation environment, simulate the process of data generation. Data can be generated by randomly generating data or by using sensors to simulate data acquisition.

Data transmission: The simulated data transmission of the USV through a communication network to a block chain node for processing and storage.

Block chain node verification: After receiving the data, the block chain node verifies the integrity of the data.

Verification result returns: The block chain node returns the verification result (pass or fail) to the USVs and stores the data on the block chain.

In the simulation environment, the data integrity protection scheme based on the block chain was tested, and 100 data transmission instances were simulated. Among which, the data passed the integrity verification 95 times. The success rate of data transmission to the block chain node was 97%. In the data integrity protection scheme based on block chain, the average data consumption time of each verification is 0.5 seconds, and the specific data is shown in Figure 2.

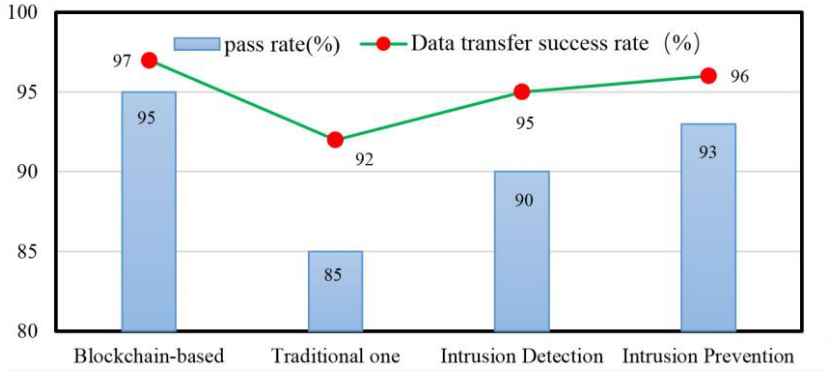

Figure 2. The results of data integrity protection based on block chain

7. Conclusion

This paper studies the application of block chain in the cyber security of USV. By introducing block chain into the communication network of USV, a decentralized trust model is realized, which provides effective protection for key links in the network such

as identity authentication, data integrity, non-repudiation and network defense. The experimental verification results show that the cyber security of USV based on block chain has high feasibility and effectiveness. This paper provides a new solution for the cyber security, which can play an important role in practical application. However, the application of block chain in the cyber security of USV still has some problems, such as performance optimization, cross-chain interoperability, etc., and further research is still needed.

References

[1] Yousef A. A., Zulkifli B. Z. A., Ahmed R. F., Hasan F. M. Z., Ahmad I. I.. Integration of Stereo Vision and MOOS-Iv P for Enhanced Obstacle Detection and Navigation in Unmanned Surface Vehicles. IEEE Access, 2023, 21(11): 128932-128935.

[2] Nelly A. S., Viktor A. S., Ruslan I. B., Elena F. A., Zoya V. A., Viktor V. M.. Intelligent Collision Danger Assessment of Autonomous Unmanned Sea-Going Vessels. International Conference on Quality Management, Transport and Information Security, Information Technologies, 2022:197-201.

[3] Ivanov Y.S., Zhiganov S.V., Ivanova T.I. Intelligent Deep Neuro-Fuzzy System Recognition of Abnormal Situations for Unmanned Surface Vehicles. International Multi-Conference on Industrial Engineering and Modern Technologies, 2019.

[4] Tuan P., Jonggyu P., Soon-Geul L., Quoc-Dong H. Adaptive Neural Network Sliding Mode Control for an Unmanned Surface Vessel. 20th International Conference on Control, Automation and Systems, 2020:519-523.

[5] Igor A., Andres U., Andrus P., and Raivo S. Simulink/MATLAB based Comparison of Neural and Basic Tracking Control for an Autonomous Surface Vessel for Situation Awareness Applications. IEEE Joint 19th International Symposium on Computational Intelligence and Informatics and 7th IEEE International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics, 2019:105-110.

[6] Xun Peng, Liu Jiaqi, Tang Zhu. Practice of edge-cloud collaboration in network security of intelligent unmanned systems, Cyberspace Security, 2024, 15(1):76-79.

[7] Agogino A. K., Holmesparker C., Tumer K. Evolving large scale UAV communication system//Proceedings of the Fourteenth International Conference on Genetic and Evolutionary Computation Conference. 2012: 1023-1030.

[8] Sachan P., Khilar P. M. Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism. International Journal of Network Security & Its Applications, 2011, 3(5): 229.

[9] Rajeshwar R., Monika S., Konda H. K., Anandhi R. J., Pravallika et al. Secured traceability System using Block Chain Technology in Supply Chain Management. 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering, 2023:532-535.

[10] Epiphaniou, G., Bottarelli, M., Al-Khateeb, H., Ersotelos, N. T., Kanyaru, J., &Nahar, V. (2020). Smart distributed ledger technologies in Industry 4.0: Challenges and opportunities in supply chain management. Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, 319-345.

[11] Ameer K. H., Shahad S. A proposed methodology to use a Block-chain in Supply Chain Traceability. 4th International Iraqi Conference on Engineering Technology and Their Applications.2021:313-317.

[12] LI Nan, Chen Lian, Pang Yanpeng, Yu Kaibo, He Yuanling et al. Analysis on key technologies evolution and application of USV. Ship Science and Technology, 2019, 41(23):29-34.

[13] Wang Biao, LI Bo, Gao Min, Qin Licheng. Review of Cooperative control strategies for unmanned ships. China Water Transport (Second Half of the Month), 2019, 19(02):3-5.

[14] Wang Wenhao, Yao Zhenxing, LI Zhipeng, Pang Hailong, Zhang Yan. Application of unmanned combat system in landing scenario. Aerospace Missiles, 2018(03):33-35.

[15] Nie Junfeng, Chen Xingjun, Shi Hongquan. Dynamic hypernetwork model for mission-driven Marine formation cloud combat system. Acta Armamentarii, 2021, 42(11):2513-2521.

[16] Wan Huijun, Cai Quanwang, Huang Zhihua. The key technologies about marine unmanned trunking communication network. Ship Science and Technology, 2022, 44(21):69-72.

[17] Zi Wenjiang. Research on Multi-USV Cooperative Obstacle Avoidance Technology Based on Fish Swarm Effect. South China University of Technology, 2020.

[18] YE Lijun, Li Kai, Ren Rui, Lian Yue. The application of block chain technology in the cooperative communication of USVs formation. Ship Science and Technology, 2023, 45(3): 56-60.