Journal of Marine Science and Technology

Volume 32 | Issue 2 Article 6

A Novel Identity Authentication Mechanism for Unmanned Maritime Vessels Communication Based on MITRE ATT&CK Framework

Junxian He
Dept. of Computer Science and Information Engineering Tamkang University New Taipei City, Taiwan

Shih-Hao Chang
Dept. of Computer Science and Information Engineering National Taipei University of Technology Taipei City, Taiwan, sh.chang@ntut.edu.tw

Recommended Citation
He, Junxian and Chang, Shih-Hao (2024) "A Novel Identity Authentication Mechanism for Unmanned Maritime Vessels Communication Based on MITRE ATT&CK Framework," *Journal of Marine Science and Technology*: Vol. 32: Iss. 2, Article 6.
DOI: 10.51400/2709-6998.2736
Available at: https://jmstt.ntou.edu.tw/journal/vol32/iss2/6

REVIEW

A Novel Identity Authentication Mechanism for Unmanned Maritime Vessels Communication Based on MITRE ATT&CK Framework

Jun-Xian He [a], Shih-Hao Chang [b,*]

[a] Dept. of Computer Science and Information Engineering, Tamkang University, New Taipei City, Taiwan
[b] Dept. of Computer Science and Information Engineering, National Taipei University of Technology, Taipei City, Taiwan

Abstract

With the development of the smart shipping industry, unmanned vessel technology is rapidly evolving, accompanied by a demand for robust Internet of Things (IoT) communication security practices. Key communication technologies for the operation of unmanned vessels include external vessel communication. One crucial aspect is the verification of the identities of the parties involved in these communication systems, as this ensures secure and trusted interactions between unmanned vessels and port management authorities. Identity authentication plays a vital role in ensuring the secure communication of unmanned vessels. This paper aims to analyze potential risks related to identity authentication technology in unmanned vessel communication systems. To effectively address these risks, we propose leveraging digital certificates and blockchain technology to achieve device non-repudiation and substitution. Based on this technology, we organize and implement defense strategies using the MITRE ATT&CK framework. This framework provides a comprehensive and systematic approach to understanding potential threats and designing appropriate defense measures. By utilizing this framework, security teams can better comprehend vulnerabilities and formulate effective countermeasures. To validate the effectiveness of the proposed defense framework, we conducted simulation experiments. These experiments helped us evaluate the efficiency and reliability of the strategies in real-world scenarios. Through these experiments, we could ascertain whether the countermeasures effectively mitigated the identified risks and ensured the secure communication of unmanned vessels.

Keywords: Unmanned ship, Internet-of-Things, Certificate, Authentication, MITER ATT&CK, UUID

1. Introduction

In recent years, there have been significant advancements in the integration of communication technology, ship design, construction, and safety technology in the shipping industry. The use of marine satellites enables real-time monitoring of operating data from the ship's engines, controllers, and various navigation equipment at a control center on land [1]. With the help of artificial intelligence (AI), a new generation of "autonomous ships" is emerging. The term Maritime Autonomous Surface Ship (MASS), also known as an unmanned ship, was coined during the 99th meeting of the United Nations International Maritime Organization (IMO) and the Maritime Safety Committee (MSC) in 2018. According to the IMO, an autonomous ship is a vessel that utilizes artificial intelligence to achieve control without the need for onboard personnel. It can be remotely controlled by shore personnel or navigate automatically based on mission requirements and environmental conditions [2].

The concept of "autonomous smart ships" primarily relies on the development of sensing, artificial intelligence, wireless communication, and

Received 10 December 2023; revised 29 March 2024; accepted 12 April 2024.
Available online 11 July 2024

* Corresponding author.
E-mail addresses: 610414020@gms.tku.edu.tw (J.-X. He), sh.chang@ntut.edu.tw (S.-H. Chang).

https://doi.org/10.51400/2709-6998.2736

autonomous control technology [3]. It is hoped that in the next few years, safe remote control or autonomous navigation of unmanned ships, as well as intelligent collision avoidance capabilities, will be gradually realized. However, due to technical reliability and safety concerns, unmanned ships are currently designed for offshore or shore navigation. Autonomous smart ships can be utilized in various civil fields such as marine data collection, environmental monitoring, fire protection, transportation and replenishment, and scientific research. They can also be utilized in national defense fields including reconnaissance and patrol, mine clearance and laying, and anti-submarine operations. Some advantages of autonomous smart ships include saving manpower, reducing the risk associated with manned operations, lowering the cost of purchasing highly-manned ships, and increasing work flexibility and efficiency.

The key communication technologies to enable the operation of unmanned ships include external communication methods such as satellite communication and communication with the shore control center, as well as autonomous path planning [4]. Internal communication methods such as environmental perception and autonomous engine room data communication, automatic obstacle avoidance, and autonomous bridge and engine room technologies are also important. Additionally, improving energy efficiency, reducing greenhouse gas emissions, and enhancing the digital control capability of power systems [5] are crucial for autonomous ship operation. The use of pure electric power or fuel-electric hybrid power propulsion systems is essential for the development of unmanned ship technology. Fig. 1 illustrates these important projects. Furthermore, we have categorized the network of future autonomous smart ships as follows (see Fig. 2):

The International Maritime Organization (IMO) published "Maritime Cyber Risk Management in the Security Management System" on January 1, 2021, in order to manage maritime cybersecurity [6]. It is evident that in the future of maritime autonomous smart ship systems, the system and network security within the ship will become an important and necessary consideration. However, since a ship may have 700 to 900 pieces of propulsion control, steering, navigation, and communication equipment, and these equipment are supplied by 80−100 manufacturers, it is crucial to have the capability to identify and understand the issues and network threats of equipment systems on autonomous smart ships provided by manufacturers [7]. In this regard, the high-simulation autonomous ship internal network and communication simulation platform in this project allows students to learn the network behavior and communication characteristics of autonomous smart ships.

With the advancement of technology in maritime unmanned ships and the Internet of Things (IoT), communication security issues have emerged alongside these technological developments. The increasing integration of new supporting technologies such as IoT and big data has exacerbated the rapid rise in cybercrime [8]. It can be observed that the vulnerability detection and attack detection system of maritime autonomous ships is a new field and challenge. Therefore, there still exists a considerable gap in information security research in this area globally. Gaining a deeper understanding of the skills, strategies, and objectives of cybercriminals is a fundamental element in establishing security infrastructure goals. Since the cyber-attack on ports in 2020, maritime-related organizations such as shipyards, shipowners, the International Maritime Organization (IMO), and classification societies in various countries have successively announced laws and regulations regarding ship cybersecurity [9]. The autonomous ship vulnerability detection platform will be

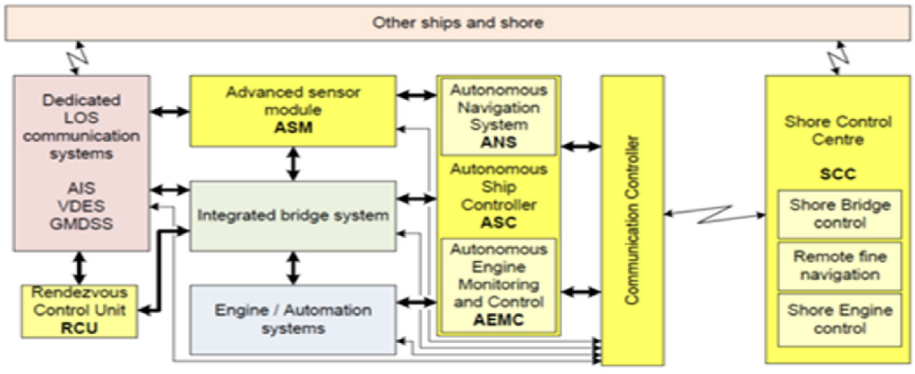

Fig. 1. Smart ship classification.

utilized to test the functionality and stability of autonomous ship industrial control equipment and to understand firmware vulnerabilities in the system. As for the last part of network attacks, we believe that conducting this project based on the MITER ATT&CK framework [10]. For network attacks can allow students to gain a comprehensive understanding of network attacks and enhance the network and system detection capabilities of future autonomous smart ships in China.

Identity authentication plays a crucial role in IoT security. With an effective identity authentication mechanism, the safety of devices and users within the IoT system can be ensured, mitigating potential risks and threats. This provides a robust security foundation for the sustainable development of IoT technology. Therefore, in this paper, we will focus on the identity authentication aspect of communication in ships. We will simulate and describe, within the MITRE ATT&CK framework, the process and techniques attackers use to attack identity authentication technologies during communication. Additionally, we will summarize defense methods and solutions to address these attacks.

The remaining parts of this paper are organized as follows: Section II provides a brief review of the background. Section III describes the system architecture of the research method and related work. Our experimental environment deployment and Experimental data will be presented in Section IV, and finally, Section V discusses the conclusions and future work.

2. Background

2.1. IoT and authentication

The Internet of Things (IoT) is a network formed by a large number of intelligent devices and sensors interconnected with each other. These devices are capable of sensing, collecting, and exchanging data, and they communicate with other devices and systems through the Internet. On the other hand, industrial control devices are used to control and monitor industrial processes and typically include components such as sensors, actuators, and controllers [11]. These devices play a crucial role in industries such as manufacturing, energy, and transportation. In the field of unmanned ship technology, IoT and industrial control devices are widely utilized in real-time communication and unmanned navigation technologies.

However, with the increasing adoption of the IoT and industrial control devices, the issue of device identity authentication has become particularly important. In the IoT, the interconnection and communication among numerous devices make device identity authentication essential. Device identity authentication ensures the security and reliability of communications, prevents unauthorized devices from accessing the network, and mitigates security risks arising from identity spoofing [12,13]. The importance of industrial control device identity authentication technology is evident in the following aspects:

A. Network Security: Once industrial control devices are connected to the Internet, they face global network attack threats. Device identity authentication ensures that only legitimate devices can access the network, preventing unauthorized access and attacks.
B. Data Security: Industrial control devices often handle sensitive data, such as production process data and energy consumption data. Device identity authentication safeguards the security of this data, preventing data tampering or theft.
C. System Integrity: Industrial control devices are typically complex systems comprising multiple components and subsystems. Device identity authentication ensures that each component and subsystem is legitimate and trustworthy, ensuring the integrity and reliability of the entire system.
D. Prevention of Malicious Operations: Authentication technology prevents unauthorized personnel or malicious software from manipulating and controlling industrial control devices, thereby preventing potential accidents or losses due to improper actions.

Therefore, in the context of IoT and industrial control devices, identity authentication technology is a crucial means of ensuring system security. Different identity authentication technologies include traditional username and password authentication, digital certificate authentication, two-factor authentication, and more [14]. With technological advancements, more advanced authentication technologies, such as biometric authentication and physical feature authentication, have emerged.

2.2. MITRE ATT&CK attack method

Recently, MITRE ATT&CK research has gained popularity for its ability to collect, analyze, and define intelligence information. Since its establishment in 2013, MITRE has gradually developed the ATT&CK framework [15], which has been well-received by

many information security vendors and enterprises. This framework provides a specific and clear common language that interprets the information security information of all parties involved. By doing so, it alleviates the burden of digesting a large amount of information for enterprises, enabling them to quickly understand the attack process and the hidden tactics, techniques, and procedures (TTP) that hackers employ to achieve their goals. The MITRE framework finds common application in various scenarios. Firstly, it is used for "attack simulation." For instance, the financial industry employs attack drills using groups like FIN6 and FIN7 to verify the effectiveness of their current defense capabilities and information security controls [16]. Secondly, it helps in "developing or deploying behavior detection and analysis technology" to assess whether the existing mechanism can detect and analyze specific targets such as account theft, privilege escalation, lateral movement, or data leakage. The third application is "Assessing SOC Maturity," which evaluates the current maturity level of a security operations center (SOC) on a scale of 1−5. The fourth is "defense gap assessment," which verifies the adherence of previously defined information security policies after significant changes like patches or infrastructure upgrades. Lastly, it facilitates the "execution of red team drills." Due to its transparency and ease of use, many companies and information security firms refer to the ATT&CK framework to plan red team drills, as all possible implementation methods and detailed processes are openly available [17].

However, this model is not effective for analyzing the adversary's individual behavior, determining the correlation between the adversary's detailed actions and tactical goals, or identifying the correlation between attack data sources and defensive countermeasures [18]. MITRE ATT&CK differs from the Cyber Kill Chain in that it maps and indexes almost everything related to intrusions by both attackers and defenders. Therefore, MITRE ATT&CK is suitable for modeling various cyber attacks. Using MITRE ATT&CK to compare the attack on the Iranian ABC and the Russian cyber attack on the US legislator, the findings are as follows: clearly divide recent cyberattacks into seven stages (①reconnaissance; ②weaponization; ③delivery; ④development; ⑤installation; ⑥command and control; ⑦targeted action); correctly express cyberattack techniques; and propose specific security measures. The MITRE ATT&CK Framework documents and categorizes cyber adversary behavior into Tactics, Techniques, and Procedures (TTPs) that are not subject to command.

2.3. Introduction to blockchain and IoT identity authentication technology

With the rapid development of the Internet of Things (IoT), secure authentication of devices and user identities has become crucial. Traditional centralized identity authentication methods in the IoT may be susceptible to single points of failure and privacy breaches. The introduction of blockchain technology provides a new approach to addressing these issues [19].

Blockchain is a decentralized, distributed ledger technology that is non-tamperable, decentralized, and transparent. These properties make blockchain an ideal solution for identity authentication. By storing the identity information of IoT devices on the blockchain, a more secure, transparent, and decentralized identity management system can be achieved. This is due to the protection of Blockchain's encryption technology and Proof of Stake (PoS) mechanism, which are achieved through the following methods:

A. In the POS mechanism, nodes confirm new blocks by participating in the consensus process. Nodes that hold more cryptocurrencies have greater rights and interests in the consensus process [20]. However, in the process of blockchain technology participating in IoT identity authentication, mining behavior does not occur and nodes do not hold cryptocurrency. Therefore, the equity value of a node is determined by the node's activity or contribution in the network. It can also be evaluated based on the node's historical behavior and reputation. In short, the rights and interests of nodes are determined based on the importance and participation of the node in the blockchain network. By rationally allocating and managing the equity value of nodes, the security and stability of the network can be ensured.
B. Data in the blockchain is usually protected through encryption technology. Each block contains the hash value of the previous block. Any tampering with the data will cause the hash value to change, thus being rejected by other nodes.

In the realm of blockchain and IoT identity authentication technology, each device or user is assigned a unique identity, recorded on the distributed ledger of the blockchain. The updating, verification, and access control of identity authentication information can be performed on the blockchain through mechanisms such as smart contracts.

This design effectively guards against identity forgery, information tampering, and unauthorized access.

Through the integration of blockchain and IoT identity authentication technology, a more secure and trustworthy IoT ecosystem can be established, providing robust support for secure communication and data sharing among devices.

2.4. Integration applications of blockchain technology with maritime communication systems

The integration of blockchain technology into maritime communication systems can bring many potential advantages to the shipping industry, including enhanced data security, identity authentication, and smart contract execution. Below are some detailed information about blockchain technology and its integration with maritime communication systems:.

2.4.1. Architecture

- Blockchain network: Maritime communication systems can build a decentralized blockchain network, where each node represents a ship or maritime equipment. These nodes can communicate through peer-to-peer network connections and have unique identity and authentication mechanisms.
- Smart contract platform: Smart contracts on the blockchain network can be used to execute various shipping business logic, such as contract management, cargo tracking, payment settlement, etc. These smart contracts can enable automated and transparent business processes in maritime communication systems.

2.4.2. Agreement details:

- Consensus protocol: Choosing a consensus protocol suitable for maritime communication systems is crucial. Depending on the network size, latency requirements and trust model, you can choose Proof of Work (PoW), Proof of Stake (PoS), or other consensus mechanisms.
- Identity authentication protocol: In maritime communication systems, the identity authentication protocol can be implemented based on the public key infrastructure (PKI) of the blockchain. Each ship or device can have a unique digital identity, verified and access controlled via smart contracts on the blockchain.
- Data transfer protocol: To ensure the security and integrity of data, maritime communication systems can use blockchain-based encryption and signature technology. Data transmission protocols can be based on traditional encryption algorithms, such as RSA, AES, etc., or new encryption technologies based on blockchain.

2.4.3. Integrated applications:

- Ship position tracking: Using blockchain technology, real-time tracking of ship position and status can be achieved to ensure the safety and credibility of ship position.
- Cargo tracking and management: Blockchain can record the source, destination and transshipment process of goods to ensure the safety and compliance of goods.
- Ship maintenance and upkeep: The process of ship maintenance and upkeep can be automated through smart contracts, improving the efficiency and reliability of ship operations.

In general, the integration of blockchain technology and maritime communication systems can bring more efficient, safer, and more trustworthy communication and business processing methods to the shipping industry. This integration can also improve the management and monitoring capabilities of maritime vessels and equipment.

2.5. UUID

UUID (Hardware Unique Identifier) is a type of identifier used to uniquely identify computer systems or devices. The primary purpose of hardware UUID is to provide a globally unique identifier, enabling the operating system and applications to recognize and track hardware devices [21].

Here are some key concepts regarding UUIDs in hardware:

A. Uniqueness: Hardware UUIDs are designed to maintain uniqueness among devices of the same model or manufacturer. This ensures that each device in the entire system has a distinct identifier.
B. Assignment Method: Hardware UUIDs are typically assigned by the device's manufacturer during production. This can be achieved through various methods, including generating based on device serial numbers, MAC addresses, or other unique hardware identifiers.
C. Fixed and Immutable: In most cases, hardware UUIDs remain fixed and immutable. Even if the

hardware configuration of a device changes, its UUID typically remains unchanged. This helps ensure that the unique identifier remains constant throughout the device's lifecycle.

D. Retrieval Method: Operating systems and applications can retrieve hardware UUIDs through corresponding APIs or commands. This enables the operating system to identify various hardware components connected to the computer and uniquely identify them based on their UUIDs.

E. Application Areas: Hardware UUIDs find widespread applications in areas such as device management, system identification, software-hardware pairing, etc. They are utilized in operating systems, drivers, and applications to ensure the unique identification of hardware devices.

F. In summary, a hardware UUID is a globally unique identifier assigned to a hardware device during manufacturing, aiding in the unique identification and management of hardware devices within a system.

2.6. Blake2

Blake2 is a hash function that is part of the BLAKE family of hash functions [22]. It is designed to provide high security, high performance, and reliability. BLAKE is a family of cryptographic hash functions that share similar structures and design concepts, but BLAKE2 is the latest, most flexible, and highest-performing member. The following is a detailed introduction to some technical concepts of Blake2:

A. BLAKE2 is designed to be a verhighly efficient hash function. It runs quickly on a variety of ous platforms and performs well with hardware acceleration. This makes BLAKE2 particularly suitable for cryptography, data integrity verification, and other applications that require fast hashing.

B. Configurability: BLAKE2 is highly configurable and can be adjusted to suit different security needs and application scenarios. It supports a variety of output lengths and uses, including hash digests, message authentication codes (MACs), pseudo-random functions (PRFs), and more.

C. Security: BLAKE2 considered many security issues when designing and adopted some advanced cryptographic technologies, such as the Merkle−-Damgård construction, shuffling function, Sponge construction, etc. Due to its strong security, BLAKE2 has been widely adopted in many security applications.

D. Parallelism: BLAKE2 takes full advantage of hardware parallelism, which enables it to perform particularly well on multi-core processors and other environments that support parallel computing. This is especially crucial when dealing with large amounts of data.

E. Collision Resistance: BLAKE2 is designed to be collision resistant, i.e. it is theoretically resistant to attacks that find two different inputs but produce the same hash output. This is an important property of hash functions in cryptography.

F. Availability: BLAKE2's open-source implementation makes it easy to integrate into a variety of applications. Due to its high performance, flexibility and security, BLAKE2 is widely used in cryptography, digital signatures, data integrity verification, blockchain and other fields.

3. Research methods and related work

3.1. Authentication

Identity authentication is a major concern in current IoT security applications. When our IoT devices engage in network communication with uncertified and risky devices, information security risks may arise. In the context of our article's topic, when ships communicate with other vessels or terminals through the maritime network, failing to authenticate the communication parties can potentially lead to data leaks and theft risks [23].

Regarding ship-to-ship communication, conventional vessels use communication software onboard. In the case of unmanned ships discussed in this article, their communication operations are carried out through the ship's own Maritime Autonomous Smart Ship (MASS) system. The MASS system relies on specific software or programs to establish communication between the client-side and the server-side of the communication receiver (and vice versa, external client-side actively connecting to the server-side of the ship's system). In this process, both communication parties must undergo identity authentication to ensure secure and valid communication (see Fig. 2).

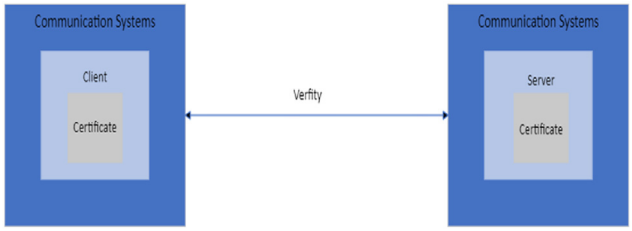

Fig. 2. Authenticate using certificates.

Although the PKI architecture is widely used for network identity authentication, it is susceptible to certain vulnerabilities. This is because Certification Authorities (CAs) may be targeted by network extortion activities, such as DNS attacks. These attacks can result in the client and server being unable to retrieve certificates issued by the CA. As a result, the identity authentication mechanism becomes ineffective, exposing devices in communication to risks [24]. Additionally, CAs are responsible for storing certificates, and if a CA is compromised, there is a risk of certificate leakage and impersonation. In severe cases, this could pose a security threat and lead to information breaches in smart manufacturing and shipbuilding.

Based on a blockchain-based architecture that is different from the traditional PKI framework, we have implemented a decentralized certificate management mechanism within the local area network. Using the PoS consensus mechanism of the blockchain, we can store and manage certificates without relying on the Certificate Authority (CA), which greatly reduces the possibility of single-point attacks on smart ship equipment. Therefore, we use a consensus mechanism to treat the certificate of each unmanned ship's communication device as a block within the network, that is, each unmanned ship's communication node. The characteristics of the blockchain ensure that once the certificate is added, it cannot be tampered with, and each block will receive a broadcast message about the certificate addition to achieve consensus management.

However, this decentralized certificate management method in the blockchain network has a shortcoming: although the blockchain network can protect certificates from tampering and attacks, it does not solve the trust problem before the device certificate is added to the network. Because the certificate of our device still needs to be issued by a CA, if an uncertified device carries an uncertified certificate into the blockchain network, it will still pose a risk to our public domain blockchain network. This means that before devices can communicate over the network, we must subject them to a trust mechanism. A device is only allowed to communicate over the network if it meets the identity criteria.

Although we can also use the PKI mechanism as the trust mechanism for certificate authentication, as mentioned above, this mechanism has shortcomings such as being vulnerable to single-point attacks and being easily imitated by CAs. Therefore, in this study, we combine the device's certificate information with some characteristics of the device that are not easily tampered with to create a universally unique identifier (UUID) unique to each device. We use this UUID for device authentication to implement a novel identity authentication mechanism. Then, we combined it with the blockchain network mechanism to form a new communication security protection mechanism.

3.2. UUID and identity authentication

In order to address the trust issue before a device joins the blockchain network, we combine the device's certificate information with certain tamper-resistant features of the device to create a universally unique identifier (UUID). In this process, we utilize the Blake2 algorithm to hash the device's features and certificate for UUID generation, using the UUID for identity verification.

Firstly, we analyze common hardware specifications of ship communication devices, identifying the MAC Address as an unchangeable device feature. For contemporary smart ships, the MAC Address only changes if the communication equipment or network card is replaced. While technologies like PUF [19], Hardware Token [20], may better serve as unique identifiers for devices, the limited hardware specifications of ship communication devices may not universally support these technologies. Conversely, any device with wireless or wired network access will inherently have a unique Mac Address. Therefore, the Mac Address can theoretically function as a unique identifier for industrial control devices.

Secondly, each digital certificate contains public key information. Taking the widely used X.509v3 format as an example, each X.509 certificate includes the public key information in the ASN.1 structure (Public Key Info), where the Public Key portion is DER-encoded. We can extract the public key information from any X.509 certificate.

Finally, to enhance the security and complexity of UUIDs, we use the Blake2b hashing algorithm to hash the MAC address and the DER-encoded public key of the digital certificate held by the node. This process generates a new UUID that serves as a unique identifier for device authentication. In this way, we can ensure that the UUID of the authenticated device corresponding to the digital certificate and MAC Address of the device is correct and unique. We verify the correctness of the UUID before the device joins the network environment to ensure that both the certificate and the device are qualified.

Once we generate the UUID, it is pre-stored in our authentication system. We utilize the pre-stored UUID as the authentication condition, and through a comparison process, authenticate the device. If the UUID is correct and meets the eligibility criteria, we proceed

with certificate verification. Only when both authentication steps pass can the system grant authentication to the device, allowing secure communication (see Fig. 3).

3.3. PKI and MITER ATT&CK

MITRE ATT&CK is a framework used to describe adversary tactics, techniques, and procedures (TTPs). ATT&CK stands for "Adversarial Tactics, Techniques, and Common Knowledge." We aim to discuss blockchain and identity authentication within the MITRE ATT&CK framework, focusing on potential tactics and techniques, along with associated processes. Our goal is to integrate our identity authentication protection mechanisms into the MITRE ATT&CK framework for discussion.

Once attackers successfully obtain the certificate private keyprivate key for the certificate, they can use it to forge certificates and impersonate legitimate entities for further attacks. Therefore, safeguarding the security of certificate private keys for certificates is crucial. MITRE ATT&CK recommends implementing measures such as encrypted storage, access controls, and key rotation to mitigate the risk of certificate private key leakage. Additionally, timely detection and response to credential access attacks are essential for protecting the security of the PKI system [25].

4. Experiment

Our goal is to implement authentication and UUID generation in the application between simulated ships and other communication stations in a simulated network environment. Simulated nodes join the blockchain network for secure storage after certificate verification, and potential attack scenarios are simulated. In this paper, we conduct simulation experiments using the NS-3 module on the Linux system (see Tables 1 and 2). During the communication process, simulated ships store node information, such as digital certificates and UUIDs, in the form of blocks at the ship's node within the field network after authentication using generated certificates and UUIDs. Subsequently, we simulate attacks on nodes based on the protection mechanisms of the blockchain and record energy consumption and runtime.

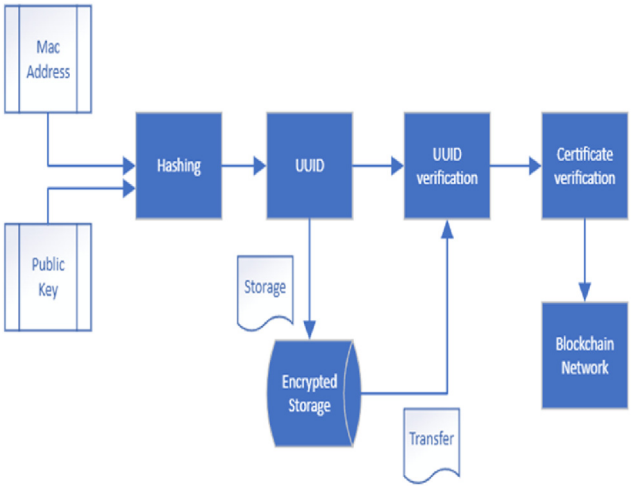

Fig. 3. The formation and application of UUID.

4.1. UUID generation application

We use the Blake2b algorithm to generate a UUID from the MAC address and the public key of the node's corresponding certificate. When performing hashing with the Blake2b algorithm, we also experimented with other hashing algorithms, namely SHA-3, SHA-2, and MD5. The results (Fig. 4) show that, under the same experimental environment, Blake2 has the fastest computing speed compared to SHA-3, SHA-2, and MD5.

After verifying the certificate, we store it in the node and utilize blockchain protection. Blocks are not only capable of storing node data but also safeguarding the confidentiality of node information. Subsequently, we simulated two scenarios: one involving a network scenario with point-to-point connections without blockchain protection, and the other involving a network scenario with blockchain protection for nodes. We compared the energy consumption data by examining the hardware resource usage in these two network scenarios:

In the above two sets of images, Test1 represents a peer-to-peer network scenario using blockchain protection technology, while Test2 represents a peer-to-peer network scenario without using blockchain protection technology. In Fig. 5, we can

Table 1. Hardware specification.

CPU	Intel(R) Core(TM) i7-10700 CPU @ 2.90 GHz
Ram	4 GB
HDD	200 GB
Network	Intel Corporation 01

Table 2. Software environment.

System	Ubuntu 18.04
Ns-3 Version	3.33
X.509 Version	V3
python	3.9.0

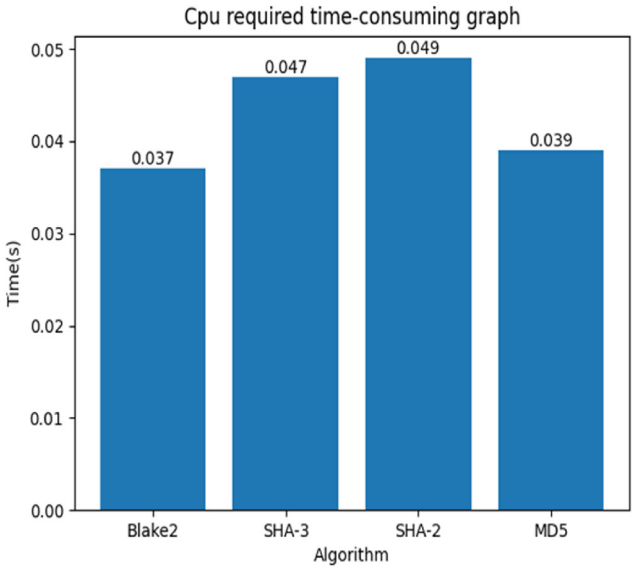

Fig. 4. CPU operation speed of different Hash algorithms.

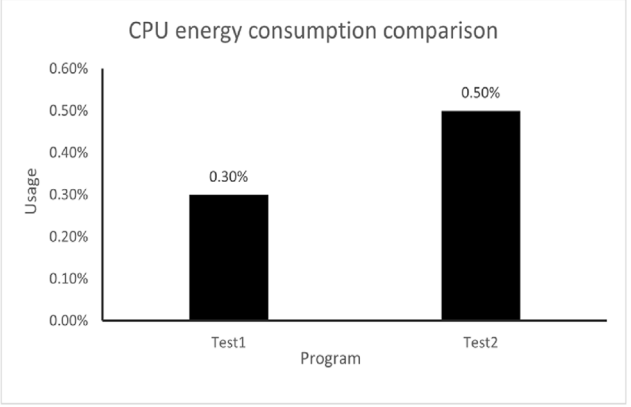

Fig. 5. CPU energy consumption comparison.

conclude that Test1 has lower CPU usage compared to the control group using Test2. However, in Fig. 6, we find that Test1 has more wake-ups per second than Test2. Nevertheless, the difference in energy consumption between the two network simulation scenarios is not very significant, which may be attributed to limitations in the hardware and software scale of the simulated scenarios.

Subsequently, we conducted node tampering attacks on the two network scenarios, Test1 and Test2. Tampering attacks involve attackers attempting to alter data in the blockchain by modifying the hash values of blocks. This type of attack poses a threat to the integrity of blockchain data, and blockchain technology is typically designed with features to resist tampering and protect data integrity.

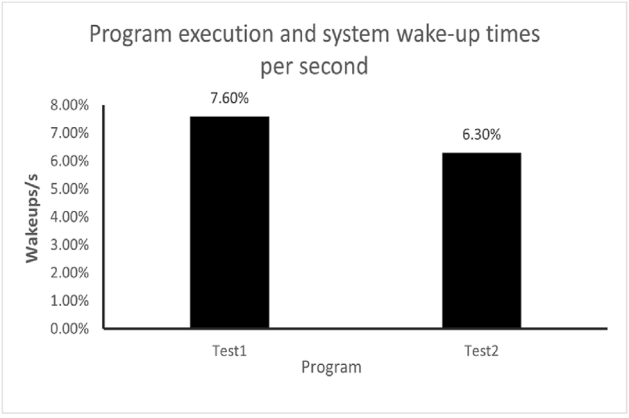

Fig. 6. Program execution and system wake-up times per second.

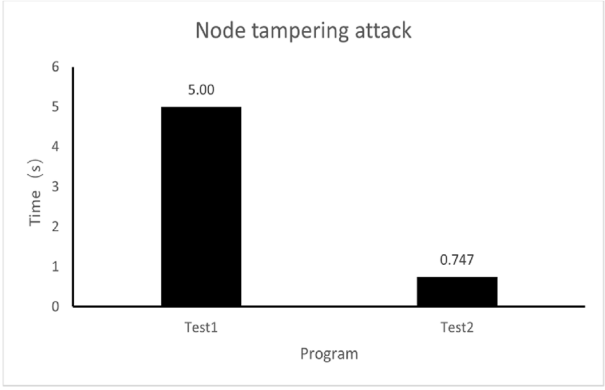

Fig. 7. Node tampering attack.

From the experimental data in Fig. 7, it is evident that the runtime of the simulated attack in Test1 is significantly higher than in Test2. In fact, the time spent on the attack in Test1 is even greater. This is because, during the experiment, the attack program encountered blocking and deadlock issues when attacking Test1. We infer that this is also due to the inability of tampering attacks to calculate hash values in a short time. In our experiment, due to the prolonged deadlock time, the program's simulation time was set to a maximum value of 5 s. This also explains why the time value for the attack program against Test1 is derived, indicating that the network scenario in Test1 has a certain resilience time when facing this type of attack. This is also in line with the MITRE ATT&CK framework's approach to resilience.

5. Conclusion and future works

In our experiments, we delved into the energy consumption differences between the blockchain network protection architecture and the traditional industrial control network architecture. While we observed that, in certain scenarios, the energy

consumption of the blockchain network did not significantly increase, this conclusion is largely contingent upon variations in the number of devices within specific domains. With the increase in devices and nodes, we speculate that the time and energy consumption required for the blockchain network to generate blocks may exhibit a gradual upward trend, necessitating further in-depth research and empirical validation.

The data and results obtained in our experiments are derived from the NS3 network simulation platform. However, NS3 struggles to handle large-scale network simulations, does not support certain complex security protocols, and lacks support for configuring complete blockchain security mechanisms. Therefore, in order to address these challenges, we require a more comprehensive network simulation platform that encompasses both technology and protocols. Once we update and enhance our experimental setup, we will proceed to utilize CALDERA and Metasploit in subsequent experimental scenarios to more effectively test the efficiency of network defense. Upon achieving the anticipated results from these simulated experiments, we will then proceed to conduct tests in real-world field environments.

In terms of identity authentication, we use the public key information of the certificate and the UUID generated by Blake2b to represent the uniqueness and tamper-proof nature of the device to a certain extent. This authentication method has obvious advantages compared to traditional unmanned ship identity authentication methods. However, in the current experiment, we did not thoroughly consider the security of this authentication method, nor did we test the potential energy consumption requirements. This was also partially limited by the experimental scenario.

Future research endeavors will focus on enhancing the authenticity of experiments by introducing more realistic network devices to simulate blockchain authentication experiments, aiming for a more comprehensive assessment of its security and usability. We plan to employ a variety of simulation attack methods, including but not limited to Denial of Service (DoS) attacks, man-in-the-middle attacks, etc., to comprehensively explore the resilience of this network security environment against attacks. Additionally, we intend to incorporate the MITRE ATT&CK framework to design methods for countering cybersecurity attacks. Through this in-depth investigation, we aim to gain a more comprehensive understanding of the practical effects of blockchain authentication in unmanned vessel networks, thereby providing robust support for the future design of secure maritime networks. This research direction not only holds the potential to actively drive the development of cybersecurity technologies in unmanned vessel networks but also promises to make significant contributions to security research across the entire Internet of Things (IoT) domain.

Conflict of interest

No potential conflict of interest was reported by the authors.

Ethics information

Written informed consent was obtained from all participants before inclusion (or publication) in this study.

References

[1] Porathe T, Prison J, Man Y. Situation awareness in remote control centres for unmanned ships. In: Proceedings of human factors in ship design & operation, 26-27 February 2014, London, UK; 2014.
[2] Wang L, Wu Q, Liu J, Li S, Negenborn RR. State-of-the-art research on motion control of maritime autonomous surface ships. J Mar Sci Eng 2019;7:438. https://doi.org/10.3390/jmse7120438.
[3] Im I, Shin D, Jeong J. Components for smart autonomous ship architecture based on intelligent information technology. Procedia Comput Sci 2018;134:91−8.
[4] Höyhtyä M, Martio J. Integrated satellite−terrestrial connectivity for autonomous ships: survey and future research directions. Rem Sens 2020;12(15):2507.
[5] Hoang AT, Foley AM, Nižetić S, Huang Z, Ong HC, Ölçer AI, et al. Energy-related approach for reduction of CO2 emissions: a critical strategy on the port-to-ship pathway. J Clean Prod 2022;355:131772.
[6] Yoo Y, Park H-S. Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. J Mar Sci Eng 2021;9(6):565.
[7] Bothur D. A comprehensive analysis of smart ship systems and underlying cybersecurity issues. 2020.
[8] Ben Farah MA, Ukwandu E, Hindy H, Brosset D, Bures M, Andonovic I, et al. Cyber security in the maritime industry: a systematic survey of recent advances and future trends. Information 2022;13(1):22.
[9] Oltedal HA, Lützhöft M. Managing maritime safety. Routledge; 2018.
[10] Park NE, Lee YR, Joo S, Kim SY, Kim SH, Park JY, et al. Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks. Comput Electr Eng 2023;105:108548.
[11] Zikria YB, Yu H, Afzal MK, Rehmani MH, Hahm O. Internet of things (IoT): operating system, applications and protocols design, and validation techniques. Future Gener Comput Syst 2018;88:699−706.
[12] Tankard C. The security issues of the Internet of Things. Comput Fraud Secur 2015;2015(9):11−4.
[13] El-Hajj M, Chamoun M, Fadlallah A, Serhrouchni A. Analysis of authentication techniques in Internet of Things (IoT). In: 2017 1st Cyber Security in Networking Conference (CSNet). IEEE; 2017.
[14] Jayalaxmi P, Saha R, Kumar G, Kumar N, Kim TH, et al. A taxonomy of security issues in Industrial Internet-of-Things: scoping review for existing solutions, future

implications, and research challenges. IEEE Access 2021;9: 25344−59.
[15] Kim K, Alfouzan FA, Kim H. Cyber-attack scoring model based on the offensive cybersecurity framework. Appl Sci 2021;11(16):7738.
[16] Noor U, Anwar Z, Amjad T, KKR Choo. A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise. Future Gener Comput Syst 2019;96:227−42.
[17] Georgiadou A, Mouzakitis S, Askounis D. Assessing mitre att&ck risk using a cyber-security culture framework. Sensors 2021;21(9):3267.
[18] Stech FJ, Heckman KE, Strom BE. Integrating cyber-D&D into adversary modeling for active cyber defense. In: Cyber deception. Building the Scientific Foundation; 2016. p. 1−22.
[19] Gao S, Su Q, Zhang R, Zhu J, Sui Z, Wang J. A privacy-preserving identity authentication scheme based on the blockchain. Secur Commun Netw 2021;2021(1):9992353.
[20] Cao B, Zhang Z, Feng D, Zhang S, Zhang L, Peng M, Li Y, et al. Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digit Commun Netw 2020;6(4): 480−5.
[21] Leach P, Mealling M, Salz R. A universally unique identifier (uuid) urn namespace. 2005.
[22] Aumasson JP, Meier W, Phan RCW, Henzen L. Blake2. The Hash Function BLAKE; 2014. p. 165−83.
[23] Ani UPD, He H, Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. J Cyber Secur Technol 2017;1(1):32−74.
[24] Dai T, Shulman H, Waidner M. Off-path attacks against PKI. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security; 2018.
[25] Ali H, Papadopoulos P, Ahmad J, Pitropakis N, Jaroucheh Z, Buchanan WJ. Privacy-preserving and Trusted Threat Intelligence Sharing using Distributed Ledgers. In: 2021 14th International Conference on Security of Information and Networks (SIN). vol. 1. IEEE; 2021.