Comprehensive Research on Cross Platform Compatibility and Security of Cryptographic Protocols in Wireless Mobile Network

Yifan Ma

School of Cryptography Engineering, University of People's Liberation Army Strategic Support Force and Information Engineering, Zhengzhou, 450004, China

Keywords: WMN cryptographic protocol; Cross-platform; Compatibility; Security

Abstract: With the increasing threats to network security, the security of cryptographic protocols in wireless mobile network (WMN) is facing severe challenges, and the cross-platform compatibility of cryptographic protocols in WMN is also an important issue. In this environment, this paper firstly summarizes the cryptographic protocols of WMN, and introduces their concepts, classifications and characteristics. Secondly, the cross-platform compatibility of cryptographic protocols in WMN is analyzed, and its influence on security is discussed. Then, the security of WMN cryptographic protocol is analyzed, and its influence on cross-platform compatibility is discussed. Finally, the relationship between cross-platform compatibility and security is discussed, and the corresponding solutions are proposed. The research in this paper has important theoretical significance and practical value, and can provide theoretical support and practical guidance for the security of wireless networks. Moreover, through the analysis and discussion of different WMN cryptographic protocols, we can find their possible loopholes and weaknesses, and put forward corresponding improvement measures to improve the security and application scope of the protocols.

1. Introduction

With the popularity of mobile devices and the rapid growth of wireless networks, people's demand for the security of wireless networks is also increasing [1]. In order to ensure the security of wireless networks, various cryptographic protocols for WMN came into being [2]. These protocols ensure the confidentiality and integrity of data by encrypting and decrypting the transmitted data, and prevent unauthorized access and attacks [3]. However, due to the possible differences between different devices and operating systems, the cross-platform compatibility of cryptographic protocols in WMN has become an important issue [4]. Moreover, with the increasing network security threats, the security of cryptographic protocols in WMN is also facing severe challenges [5].

At present, the research on cryptographic protocols of WMN mainly focuses on security, while the research on cross-platform compatibility is relatively rare [6]. However, in practical applications, the cross-platform compatibility of cryptographic protocols in WMN is equally important [7]. Based on this, this paper aims to study the cross-platform compatibility and security of cryptographic protocols in WMN, explore the relationship between these two indicators, and propose corresponding solutions. Its significance lies in that the comprehensive research on the cross-platform compatibility and security of cryptographic protocols in WMN can provide theoretical support and practical guidance for the security of wireless networks. Moreover, through the analysis and evaluation of different WMN cryptographic protocols, we can find their possible loopholes and weaknesses, and put forward corresponding improvement measures to improve the security and application scope of the protocols. In addition, this study can also provide reference for related network security standards and norms.

  DOI: 10.25236/iwmecs.2023.005

2. WMN cryptographic protocol

2.1. Concept and classification of cryptographic protocols in WMN

The WMN cryptographic protocol refers to a protocol that uses cryptographic technology to encrypt and decrypt data in order to realize the security and confidentiality of data transmission in the WMN environment [8]. According to the different encryption and decryption methods, the cryptographic protocols of WMN can be divided into symmetric cryptographic protocols and asymmetric cryptographic protocols. The implementation process of node security authentication is shown in Figure 1.

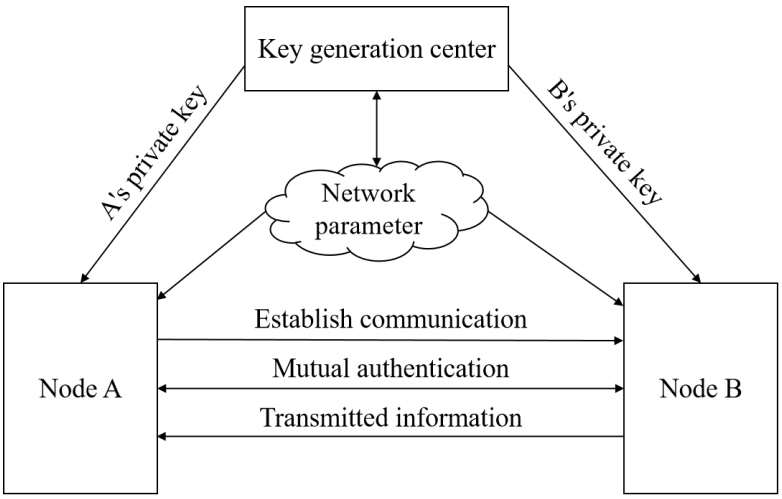

Figure 1 Implementation process of node security authentication

Symmetric cryptographic protocol refers to a cryptographic protocol that uses the same key for encryption and decryption, also known as private key cryptographic protocol. In WMN, symmetric cryptographic protocols are usually used to protect the confidentiality and integrity of data, such as WEP(Wired Equivalent Privacy) and TKIP (Temporary Key Integrity Protocol) [9]. Asymmetric cryptographic protocols refer to cryptographic protocols that use different keys for encryption and decryption, also known as public key cryptographic protocols. In WMN, asymmetric cryptographic protocols, such as RSA(Rivest-Shamir-Adleman) protocol and ECC(Elliptic Curve Cryptography) protocol, are usually used to realize identity authentication and key agreement.

2.2. Characteristics and requirements of WMN cryptographic protocol

(1) Efficiency: Due to the limited bandwidth of WMN, cryptographic protocols need to reduce the calculation and data transmission of encryption and decryption as much as possible to ensure the performance and efficiency of the network.

(2) Security: Cryptographic protocols need to ensure the confidentiality, integrity and availability of data to prevent unauthorized access and attacks.

(3) Flexibility: Because different application scenarios and network environments need different security requirements, cryptographic protocols need to be flexible and configurable to meet different requirements.

(4) Cross-platform compatibility: Because there are many different devices and operating systems in WMN, cryptographic protocols need to have good cross-platform compatibility to support secure communication between different devices.

(5) Ease of use: Because ordinary users have limited knowledge of cryptographic protocols, cryptographic protocols need to be easy to understand and use in order to improve users' acceptance and usage.

3. Research status of cross-platform compatibility

With the wide application of WMN, more and more devices are connected to wireless networks, and different devices use different operating systems and hardware platforms, so the cross-platform

compatibility of WMN cryptographic protocols has become an important research direction [10]. At present, the research on cross-platform compatibility of WMN cryptographic protocol mainly focuses on the following aspects:

(1) Research on cross-operating system compatibility: Different devices may use different operating systems, such as iOS, Android, Windows, etc. WMN cryptographic protocol needs to be able to run normally on different operating system platforms and ensure security. At present, the research mainly focuses on the support and adaptation of different operating system platforms and the use of operating system security mechanisms. (2) Research on cross-hardware platform compatibility: Different devices may use different hardware platforms, such as ARM and x86. WMN cryptographic protocol needs to be able to run normally on different hardware platforms and ensure security. At present, the research mainly focuses on the support and adaptation of different hardware platforms and the use of hardware security mechanisms. (3) Research on cross-protocol compatibility: Different application scenarios may need to use different cryptographic protocols, such as WPA2 and WPA3. WMN cryptographic protocols need to be able to support different cryptographic protocols and ensure security. At present, the research mainly focuses on the support and adaptation of different cryptographic protocols and the use of cryptographic protocol security mechanisms. (4) Research on cross-network compatibility: WMN cryptographic protocols need to be able to support different wireless network standards, such as Wi-Fi, Bluetooth, ZigBee, etc. At present, the research mainly focuses on the support and adaptation of different wireless network standards and the use of wireless network security mechanisms.

4. Present situation of safety research

At present, the security research of WMN cryptographic protocol mainly focuses on the following aspects:

(1) Research on the security of encryption algorithm: The encryption algorithm used in WMN cryptographic protocol is one of the key factors affecting its security. At present, the research mainly focuses on the analysis and evaluation of different encryption algorithms in order to find their possible loopholes and weaknesses. Moreover, some new encryption algorithms are constantly proposed and studied to improve the security of WMN cryptographic protocol. (2) Research on protocol security: The security of WMN cryptographic protocol depends on the design and implementation of the protocol itself. At present, the research mainly focuses on the analysis and evaluation of different cryptographic protocols in order to find their possible loopholes and weaknesses. For example, some studies have analyzed the security of WPA2 protocol and found some loopholes in it. (3) Research on network security: The security of WMN depends not only on the cryptographic protocol itself, but also on the network environment. At present, the research mainly focuses on the field of network security, such as security threats and attack methods of wireless networks, network security monitoring and defense technologies. These studies are helpful to improve the overall security of WMN. (4) Research on user behavior security: When users use WMN, their behavior habits will also affect the security of cryptographic protocols. At present, the research mainly focuses on the analysis and evaluation of user behavior in order to improve users' safety awareness and behavior. For example, some studies have analyzed the security risks of users in the use of wireless networks, and put forward some security suggestions.

5. Cross platform compatibility and security of WMN cryptographic protocol

5.1. Cross-platform compatibility analysis of WMN cryptographic protocol

The cross-platform compatibility of WMN cryptographic protocol means that the cryptographic protocol can run normally and ensure security under different operating systems, hardware platforms and network environments. The cross-platform compatibility of WMN cryptographic protocol needs to be analyzed and considered from many aspects. By adopting common encryption and security mechanisms, following the security norms and standards of different platforms and

protocols, and adopting modular design, the cross-platform compatibility of WMN cryptographic protocols can be realized and its security can be guaranteed.

Different devices may use different operating systems, such as iOS, Android, Windows, etc. WMN cryptographic protocol needs to be able to run normally on different operating system platforms and ensure security. In order to achieve cross-operating system compatibility, cryptographic protocols can adopt encryption libraries and security mechanisms provided by operating systems, or develop independent encryption libraries and security mechanisms. Moreover, cryptographic protocols need to follow the security specifications and standards of operating systems to ensure security on different operating system platforms.

Different devices may use different hardware platforms, such as ARM and x86. WMN cryptographic protocol needs to be able to run normally on different hardware platforms and ensure security. In order to achieve cross-hardware platform compatibility, cryptographic protocols can adopt encryption libraries and security mechanisms provided by hardware platforms, or develop independent encryption libraries and security mechanisms. Moreover, cryptographic protocols need to follow the security specifications and standards of hardware platforms to ensure security on different hardware platforms.

Different application scenarios may need to use different cryptographic protocols, such as WPA2, WPA3, etc. WMN cryptographic protocols need to be able to support different cryptographic protocols and ensure security. In order to achieve cross-protocol compatibility, cryptographic protocols can adopt modular design, and different protocols can be realized as independent modules, which can be called as needed. Moreover, cryptographic protocols need to follow the security specifications and standards of different protocols to ensure the security of different protocols.

WMN cryptographic protocols need to be able to support different wireless network standards, such as Wi-Fi, Bluetooth, ZigBee and so on. In order to achieve cross-network compatibility, cryptographic protocols can adopt general encryption and security mechanisms to adapt to different wireless network standards. Moreover, cryptographic protocols need to follow the security specifications and standards of different wireless network standards to ensure security on different wireless networks.

5.2. Security analysis of WMN cryptographic protocol

The security of WMN cryptographic protocol is the key to its design and application. Its security also needs to be analyzed and considered from many aspects. The security of WMN cryptographic protocol can be improved by choosing a secure encryption algorithm, following security norms and standards, considering network security factors, and improving users' security awareness.

The encryption algorithm used in WMN cryptographic protocol is one of the key factors affecting its security. Different encryption algorithms have different security characteristics and weaknesses, which need detailed analysis and evaluation. For example, some traditional encryption algorithms such as WEP have been proved to have serious security vulnerabilities, while some new encryption algorithms such as AES have higher security. Therefore, when choosing an encryption algorithm, it needs to be evaluated and selected according to the actual needs and security requirements.

The security of WMN cryptographic protocol depends on the design and implementation of the protocol itself. Protocol security analysis needs to analyze and evaluate the message format, encryption and decryption process, key management and so on, in order to find possible loopholes and weaknesses. For example, some studies have analyzed the security of WPA2 protocol and found some loopholes in it. Therefore, when designing and implementing WMN cryptographic protocol, it is needed to follow the security specifications and standards to ensure the security of the protocol.

The security of WMN depends not only on the cryptographic protocol itself, but also on the network environment. Network security analysis needs to analyze and evaluate the security threats and attack means of wireless network, network security monitoring and defense technology, etc., in order to improve the overall security of WMN. For example, some studies have analyzed the

security threats and attack methods in wireless networks, and put forward some defensive measures. Therefore, when designing and implementing WMN cryptographic protocol, we need to consider network security factors and take corresponding defense measures.

When users use WMN, their behavior habits will also affect the security of cryptographic protocols. User behavior security analysis needs to analyze and evaluate users' behavior habits in order to improve users' safety awareness and behavior. For example, some studies have analyzed the security risks of users in the use of wireless networks, and put forward some security suggestions. Therefore, when designing and implementing WMN cryptographic protocol, it is needed to consider user behavior factors and provide corresponding security suggestions and guidance.

5.3. Relationship between cross-platform compatibility and security

Cross-platform compatibility and security of WMN cryptographic protocol are two important indicators, and there is a certain relationship between them. When designing and implementing this protocol, it is needed to comprehensively consider and evaluate these two indicators in order to find the best balance point and ensure the security and application scope of the protocol. First of all, we should consider the impact of cross-platform compatibility on security. The cross-platform compatibility of WMN cryptographic protocol means that it can run normally in different operating systems, hardware platforms and network environments. This compatibility can improve the application scope and utilization rate of the protocol, but it may also bring some security problems. For example, on different operating system platforms, the implementation of the protocol may be different, which leads to security vulnerabilities. Therefore, when designing and implementing WMN cryptographic protocol, we need to consider the influence of cross-platform compatibility on security, and take corresponding measures to improve security. The data processing platform is deployed as shown in Figure 2.

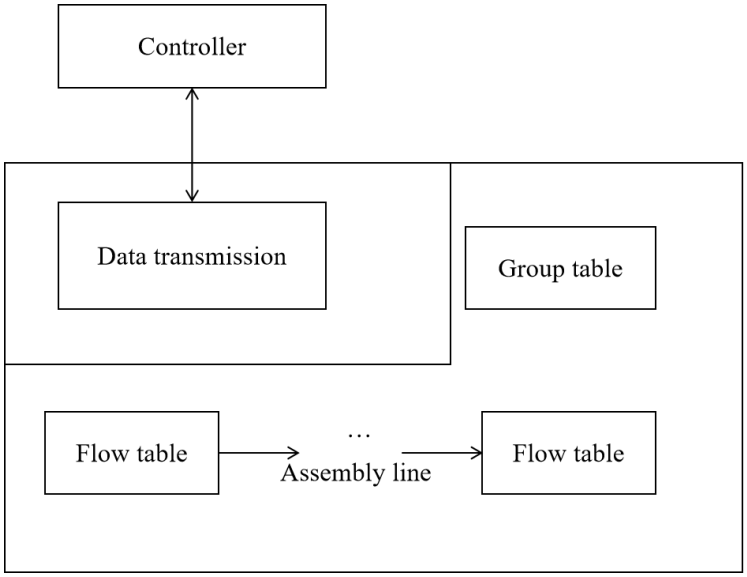

Figure 2 Deployment of data processing platform

Secondly, we should consider the influence of security on cross-platform compatibility. The security of WMN cryptographic protocol is the key to the design and application of this protocol, and security may also have an impact on cross-platform compatibility. For example, in order to achieve higher security, the protocol may adopt some special encryption and security mechanisms, which may not work properly on some operating systems or hardware platforms. Therefore, when designing and implementing WMN cryptographic protocol, we need to consider the influence of security on cross-platform compatibility, and take corresponding measures to ensure the cross-platform compatibility of the protocol. Finally, the balance between cross-platform compatibility and security. Cross-platform compatibility and security of WMN cryptographic protocol are two mutually influencing indicators, which need to be balanced in design and

implementation. On the one hand, it is needed to ensure the cross-platform compatibility of the protocol to improve the application scope and utilization rate of the protocol; On the other hand, we should ensure the security of the protocol to prevent the occurrence of security vulnerabilities and attacks. Therefore, when designing and implementing WMN cryptographic protocol, it is needed to comprehensively consider and evaluate cross-platform compatibility and security in order to find the best balance point.

6. Conclusions

With the continuous growth of new technologies such as Internet of Things and cloud computing, the application scenarios of WMN are becoming more and more extensive. In these scenarios, the cross-platform compatibility and security issues of WMN cryptographic protocol are more prominent. Because different devices and operating systems may be different, if the protocol does not have good cross-platform compatibility, it may lead to data transmission security problems. Based on this, this paper aims to study the cross-platform compatibility and security of WMN cryptographic protocol, discuss the relationship between these two indicators, and propose corresponding solutions. By analyzing and evaluating different WMN cryptographic protocols, we can find their possible loopholes and weaknesses, and put forward corresponding improvement measures to improve the security and application scope of the protocols. Generally speaking, the research results of this paper can provide theoretical support and practical guidance for wireless network security, and can also provide reference for related network security standards and norms. It has important theoretical significance and practical value, and can provide theoretical support and practical guidance for the security of wireless networks.

References

[1] Li Yanan, Xiao Meihua, Li Wei, et al. Security Proof of Wireless Mesh Network Authentication Protocol Based on Event Logic [J]. Computer Engineering and Science, 2017, 39(12):9.

[2] Che Bubo, Guo Gaizhi. Research on transmission efficiency and security of wireless sensor network protocol TEEN [J]. Journal of Chongqing Institute of Science and Technology: Natural Science Edition, 2018, 20(1):5.

[3] Sun Yanan, Chang Xinfeng. Research on the Security of Flood Time Synchronization Protocol in Wireless Sensor Networks [J]. Electronic Design Engineering, 2017(3):5.

[4] Zhu Xiaoming, Liu Bei, Bai Xiang, et al. Research on wireless blockchain security of CSMA/CA network protocol [J]. Journal of Chongqing University of Posts and Telecommunications: Natural Science Edition, 2022, 34(1):6-15.

[5] Wang Guangjie, Guo Andong, Gong Luyan, et al. Realization of cross-platform compatibility of mobile terminals [J]. Petroleum Planning and Design, 2017, 28(1):5.

[6] Lu Ya. Token-based privacy protection and authentication protocol for WMN [J]. Computer Applications and Software, 2019, 36(5):6.

[7] Yu Yang. Research on the security measurement method of hospital wireless network information nodes [J]. Automation and Instrumentation, 2020(1):4.

[8] Ke Fenfen. Research on the security of cross-platform mobile application development technology [J]. Wireless Internet Technology, 2020, 17(5):2.

[9] Liu Bin, Wang Meng, Li Lixin, et al. Physical layer security of wireless networks [J]. Mobile Communications, 2019, 43(10).

[10] Lin Xi 'er. Security performance analysis and optimization of WEP protocol in wireless networks [J]. Information Weekly, 2019(12):2.