Network Security Protocol Testing Technology Based on Wireless Communication System

Jinyun Yu[1*], Hao Sun[2] and Tuteng Chen[2]

{*Corresponding author: chentuteng@im.ehv.csg}
{ yujinyun@um.ehv.csg, mesuihao@foxmail.com}

[1]Dali Bureau of CSG EHV Transmission Company, Dali 671000, China

[2]Kunming Bureau of CSG EHV Transmission Company, Kunming 650217, China

Abstract: Network security protocol (NSP) TT has become a hot topic of research nowadays. This paper researches NSP testing technology(TT) based on Wireless Communication System(WCS), briefly analyzes wireless collaborative communication methods and NSP TT, including encryption and signature protocols and network security communication protocol execution process; designs an adaptive black-box testing method for stream cipher and group cipher, which are commonly used in wireless communication networks, and uses the designed testing scheme to design The test system and cryptographic test system architecture of wireless communication NSPs are designed using the designed test scheme, and the implementation of the system is modularized and the corresponding test results are analyzed. The results of the experimental tests show that the NSP testing technique based on WCS is feasible.

Keywords: Wireless Communication System, Network Security, Network Testing, Testing Technology

1. Introduction

Wireless communication network is a hot research area of international attention and is the core of the national key construction of information technology Internet of Things. As a new type of network, it is necessary to have sufficient security mechanisms to guarantee the security of applications, so the security of wireless communication networks has become one of the research priorities. There are already many algorithms and security protocols suitable for the characteristics of wireless communication networks, but whether these protocols meet the correctness and security in the implementation stage is an important factor affecting the security performance of the network, which needs to be tested to verify the implementation of the protocols. In this paper, NSP testing techniques are studied mainly based on WCSs.

Regarding NSP testing techniques for WCSs, many scholars at home and abroad have researched and analyzed them.Johannis W reached a preliminary consensus in the important areas of user, data and update management as well as network connectivity and user friendliness, optimizing user management by connecting to

ICSETPSD 2023, November 17-18, Coimbatore, India

DOI 10.4108/eai.17-11-2023.2342823

directory services and defining access control, combining patient data economy on analyzers with data and data transfer encryption and technically secure communication protocols, update management needs to be defined according to the contract [1].Putra E G R study found that public key algorithms are commonly used to negotiate session keys and authenticate among communicating parties, and then the consensus session keys of the parties are used in a symmetric algorithm for the communication of confidential information [2].

Although a complete cryptographic algorithm(CA) includes three processes: encryption, transmission, and decryption, the CA itself is mainly concerned with the design of encryption and decryption algorithms. In this paper, we analyze the testing requirements of wireless communication NSPs, and propose a black-box testing scheme for wireless communication NSPs based on consistency testing, which can test the security protocols of wireless communication networks and the pseudo-random numbers used in the protocols, so as to obtain the evaluation of the services and security functions implemented by the security protocols and realize the NSPs of WCSs The study of testing techniques for NSPs in WCSs [3-4].

The main content of the article is as follows:

In the first part, the background and significance of network security protocol testing technology based on wireless communication systems.

In the second part, WCS and NSP TT include methods for wireless collaborative communication.

In the third part, wireless communication, including security issues of wireless communication networks.

In the fourth part, experimental analysis of wireless communication network security protocol testing technology.

In the fifth part, the conclusion includes the limitations of the research and future research directions.

2. WCS and NSP TT

2.1 Wireless Collaborative Communication Method

In collaborative communication, the source first sends signals carrying its own information to the host and the relay, which processes the received source signals according to a specific collaborative approach and then forwards them to the host. The host combines and decodes all the received signals according to certain decoding rules to recover the information sent by the source. The basic collaboration methods can be generally grouped and classified according to the signal processing method and the source of the forwarded signal [5].

According to the different processing of the relay for the forwarded signal, collaborative communication can be divided into decoding forward, amplifying forward, and coding collaboration. The advantage of decode-ahead transmission is that it has low complexity and the relay requires only simple hard judgments, which can eliminate the accumulation of background noise and achieve good performance at high signal-to-noise ratios [6]. However, when the relay is unable to correctly adjudicate the source signal, its forwarding signal can cause an error propagation effect, which affects the diversity gain of the system. To solve this problem, an

adaptive hybrid decoding forwarding scheme is given, i.e., the relay performs decoding forwarding only when the source signal is correctly received; otherwise, the system falls back to the non-collaborative mode.

The relay receives and stores the analog waveform from the source, then amplifies it directly and sends it to the host. The host merges the signals from the source and the relay directly and then adjudicates them. Although the relay amplifies the analog waveform with the background noise in it, the signal provides independent fading samples of the source information at the signal host as well, and thus is able to bring diversity gain to the system [7-8]. A detailed analysis of the amplified prepass collaboration under two collaborative user assumptions demonstrates that the collaboration is capable of achieving full diversity at high signal-to-noise ratios. Compared to decoding prepass, amplifying prepass requires additional storage units in the relay for the analog waveforms, which increases the complexity. In addition, the source-to-relay channel gain needs to be known to calculate the optimal merging coefficients when the waveforms are merged by the signal host, so this collaboration approach needs to be coupled with the design of the corresponding channel estimation and feedback mechanisms [9].

2.2 NSP Testing Techniques

2.2.1. Encryption and signature protocols

An encryption protocol is a protocol that, given an encryption algorithm, specifies the steps to be performed by the communicating parties and the order in which each step is to be performed, thus ensuring the smooth implementation of the encryption algorithm. The signature protocol is designed to ensure the smooth implementation of the signature algorithm. The current mainstream encryption algorithms are divided into two categories according to whether the encryption and decryption algorithms use the same key: symmetric encryption/signature algorithms. Symmetric algorithms often require each pair of communicating parties to keep an identical key between them, and public-key algorithms communicate parties normally only need to keep their own private keys and the public keys of the other party they expect to communicate with. In large networks, the number of keys that each communicating entity needs to keep is relatively small when using public-key algorithms, and it is simpler and more convenient for users to manage the keys [10]. And in general, the speed of encryption and decryption operations of public key algorithms is one to several orders of magnitude slower than that of symmetric algorithms. Therefore, in practical communication protocols, these two types of algorithms are often used jointly to complement each other's strengths and weaknesses.

2.2.2. Network security communication protocol execution process

The execution process of a two-party secure communication protocol with a mix of public keys and symmetric algorithms and only one sender and one receiver. The sender and receiver each select a portion of the session key and then encrypt it with the other party's public key. After receiving the encrypted message from the other party, both parties decrypt it with their own private keys and then compute the common session key. The session key is dedicated for subsequent confidential communication and needs to be renegotiated the next time communication is required [11-12]. And the subsequent multiple interactive confidential communications are encrypted and

decrypted using the common session key. This enables efficient communication of confidential information and eliminates the need to keep the session key in the usual way. If the public key signature of the communicating entity is added in, the formed verifiable confidential communication protocol[13].

3. Wireless Communication NSP TT

3.1 Security Issues of Wireless Communication Networks

Wireless Communication System refers to a way to achieve communication through wireless protocols.

Wireless communications include a variety of fixed, mobile and portable applications such as two-way radios, mobile phones, personal digital assistants and wireless networks. Other examples of radio wireless communication are GPS, garage door remote control, wireless mouse, etc.

Most wireless communication technologies use radio, including Wi-fi, which is only a few meters away, and deep space networks, which communicate with Voyager 1 over millions of kilometers. However, some wireless communication technologies do not use radio, but use other electromagnetic wave wireless technologies, such as light, magnetic fields, electric fields, etc.

Because the characteristics of the communication network itself make WCSs more vulnerable to damage, WCSs need to resist various security attacks and threats when dealing with specific tasks, and the security, confidentiality, and reliability of data need to be guaranteed. Although the standards of WCSs for security differ slightly in the face of different domains, such as military and civilian domains, the security objectives of WCSs can be broadly divided into:

Integrity. In the transmission process, due to network signal reasons or received a hacker attack, may corrupt the data message and make it lose some data, when the data integrity to ensure that the information will not be tampered with, to ensure that the original information can be received intact, and not to lose any data.

Confidentiality. Confidentiality will ensure that confidential data will not be leaked to other individuals or collectives. Once an attacker gets access to highly sensitive information transmitted by the communication network, such as routing information, key management information, etc., then the security of the whole network will not be guaranteed.

Availability. The availability is such that when the network faces various network attacks, so that the attacks do not affect the main functions of the WCS, the network can still perform its basic tasks and the attacks do not cause the overall functions of the network to be unachievable. In addition the proposed security protocols should not limit the availability of the network and be able to defuse the network attack while maintaining the normal operation of the system.

Freshness. Freshness ensures that users get the desired information quickly. When subject to replay attacks, to avoid receiving duplicate messages all the time, the process of establishing the key requires that the key shared by both parties is up-to-date, which ensures that the message is sent to the receiver immediately after it is generated and is not affected by duplicate messages.

Non-repudiation. Non-repudiation means that the information one sends cannot be

denied by the sender of the information source. Preventing attackers from impersonating their identities to send malicious attacks can be achieved through signatures, ID cards, access control, and other security goals that can achieve non-repudiation.

3.2 NSP Testing Techniques based on WCSs

As shown in Figure 1, for the collaborative multiple access channel, the whole communication process is divided into three time slots, and in the ith time slot, the source Si broadcasts to the host E. Then the received signals in the relay R and the host E can be expressed as follows, respectively

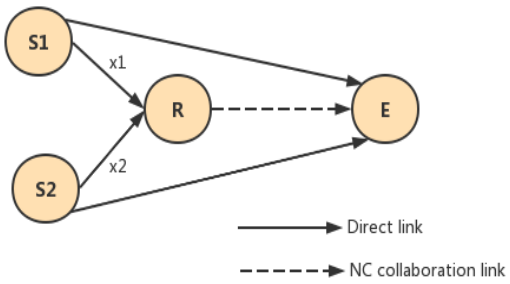

Fig.1 A network coding system model for multiple access channels

$$y_{ir} = h_{ir}\sqrt{p}x_i + n_{ir}, i = 1,2 \quad (1)$$

$$y_{ie} = h_{ie}\sqrt{p}x_i + n_{ie}, i = 1,2 \quad (2)$$

Where y_{ir} and y_{ie} denote the received signals of R and E, respectively, h_{ir} and h_{ie} denote the channel gains from S_i to R and E, respectively, n denotes additive Gaussian white noise, and p is the average transmit power. The channel is assumed to be frequency non-selective Rayleigh block fading model. The relay R performs MLD judgments on the received signal y_{ir} to obtain $\hat{x}_i$.

$$\hat{x}_i = sign(\mathrm{Re}(h_{ir}^* y_{ir})), i = 1,2 \quad (3)$$

It is then heterogeneously combined into $\hat{x}_\oplus = \hat{x}_1 \oplus \hat{x}_2$, and determines the weight factor β with a specific algorithm to adjust the transmit power to forward it. Thus, at the 3rd time slot, the signal received by the signal host E can be expressed as

$$y_{re} = h_{re}\sqrt{ap}\hat{x}_\oplus + n_{re} \quad (4)$$

The merging operation makes the signals correlated with each other, so the joint

MLD is used in the signal host D to estimate the sent symbol pair $x = (x_1 + x)_2$

$$\hat{x} = \arg \min_{\hat{x}_i \in \{-1,1\}} \left(\sum_{i=1}^{2} \left| \mathrm{Re}(h_{ie}^* y_{ie}) - |h_{ie}|^2 \sqrt{p} \hat{x}_i \right|^2 + \left| \mathrm{Re}(h_{ie}^* y_{ie}) - |h_{ie}|^2 \sqrt{p} \hat{x}_{\oplus} \right| \right) \tag{5}$$

In the above link adaptive network coding transmission scheme, the reliability critically depends on whether the weighting factor a can accurately indicate the signal quality. In this paper, we use LLR to estimate the signal quality and use it to adjust a to improve the accuracy of the adaption.

4. Experimental Analysis of Security Protocol Testing Techniques for Wireless Communication Networks

4.1. Security Protocol Test System Design

Both the wireless communication NSP test system and the cryptographic test system are conducted in a black-box environment, so their structural design is described together in this section.

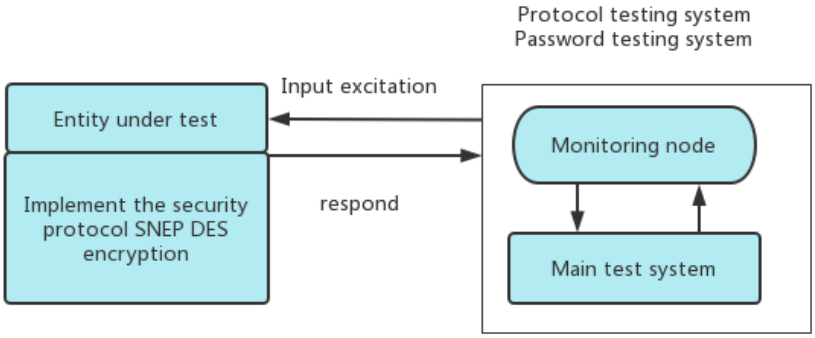

Fig.2 Test system structure diagram

The structure of the test system designed in this paper is shown in Figure 2. The test system uses the monitoring node (for sending and receiving packets from the tested node/network) to input excitation to the tested entity, which responds and transmits the packets to the test system; the monitoring node communicates both the sent and received data to the main test system through the serial port, and the main test system needs a serial communication module to process the serial information; the main test system completes the main test and judgment functions. including serial communication module, display module, randomness test library several parts, protocol test system also need to have a consistency test module (to judge the consistency of the protocol), password test system has a password test module.

4.2. Implementation of Security Protocol Testing System for Wireless Communication Networks

This section describes the modular implementation of the system based on the structure of the test system for security protocols of wireless communication networks. The security protocol test system is divided into two major parts:the monitoring node and the main test system. The test procedure of the monitoring node is done on the GAINZ node of the Institute of Computing, Chinese Academy of Sciences, and the main test system is implemented in VC6.0.

4.2.1. Monitoring node implementation

The main function of the monitoring node is to communicate with the entity under test, receive the data packets output by the entity under test, parse them and send them to the main test system. The monitor node program is mainly responsible for the communication process between GAINZ node and CC2420, to ensure the normal communication process between the nodes.

4.2.2. Monitoring node workflow

The monitoring node uses the function void handlepacket(void) to complete the judgment and processing of data, if it is a correct response packet, it sends the data to the main test system through the serial port, if it is not correct, it takes the retransmission mechanism and asks to resend it. the operating system of the development environment accompanying the GAINZ node is the GOS operating system designed by the Institute of Computing, Chinese Academy of Sciences, which can It is able to complete basic task scheduling and management.

4.3. Discussion

Network security protocol testing technology based on wireless communication system is one of the important means to protect wireless network communication security. It improves the security of the wireless communication system by fully testing and evaluating the network security protocol, and discovering the potential vulnerabilities and security risks. At present, the network security protocol testing technology mainly focuses on the wireless LAN and the mobile communication network. However, with the rapid development of the Internet of Things and the diversified application of wireless communication technologies, the coverage of such test technologies in other fields (such as the Internet of vehicles, health care, etc.) is small. Network security protocols for wireless communication systems are often very complex, and the testing process requires a lot of time, resources, and expertise. In addition, the hardware equipment and software tools required for testing can also be expensive, making the test more expensive. With the continuous evolution of hacking technology and cyber attack means, cyber security protocol testing technology needs to timely follow up and respond to new security threats. However, in some cases, testing techniques may fail to detect new attack vulnerabilities in time.

Network security protocol testing techniques are often used to evaluate the security of WLAN networks, including WiFi networks and enterprise-class wireless networks. Through the test of the security protocol, the potential risks such as password cracking, middleman attack and replay attack can be found. It is also applicable to evaluate the security of mobile communication networks, such as 4G and 5G

networks. These tests can reveal the possible problems of eavesdropping, camouflage, information tampering and so on in the transmission process. With the popularity of the Internet of Things, the network security protocol testing technology has also been gradually applied to the Internet of Things devices and systems. It can evaluate the security of sensor nodes, control platforms, and communication channels and provide patch suggestions.

We should focus on broadening the application scope of testing technology, covering more areas and application scenarios. To reduce the complexity and cost of testing, automated and intelligent tools can be used to speed up the testing process and improve the efficiency of discovering potential security vulnerabilities. Using machine learning and artificial intelligence technology, abnormal behavior and attack patterns can be identified in advance. The rapid evolution of forms of cybersecurity attacks requires testing technologies to achieve continuous security monitoring and vulnerability scanning. Conduct regular security assessment and vulnerability repair to maintain the security state of the wireless communication system.

4.4. CA Test System Implementation

This section describes the implementation of a CA test system for wireless communication NSPs, which was developed on a Windows platform using VC6.0 tools. The main implementation is to judge the type of password used in the entity under test and then test the different patterns separately.

4.4.1 Password testing system implementation

The main functions of the testing system for CAs:To judge the encryption mode of the protocol entity under test, the randomness test is mainly taken for stream ciphers, and the randomness test and avalanche characteristic test, plaintext correlation test, and linear performance test are performed for group ciphers. The test results are saved in the output file.

4.4.2 Analysis of test test results

Using the CA testing system for wireless communication networks implemented in this paper, black-box tests are conducted on entities that have implemented the DES encryption algorithm. The test results and analysis are as follows.

(1) Randomness test

The randomness test has been described in the previous protocol test system, so we will not repeat it here and only analyze the results of the test. When the entity under test uses a fixed key, only a few test items can pass; when the entity under test uses a pseudo-random number with good randomness as the key, only the discrete Fourier and general statistics tests fail. This indicates that the performance of the ciphertext generated by DES encryption algorithm and the randomness of the key are highly related.

(2) Avalanche test results and analysis

The results of the avalanche test on the DES encrypted data of the tested entity are shown in Table 1 below.

Table 1. Test Results of Strict Avalanche Characteristics of DES

Number of tests	Maximum probability	Minimum probability

10000	0.517900	0.481700
20000	0.515230	0.485800
30,000	0.512100	0.486547
40000	0.511480	0.495000
50,000	0.504950	0.490700

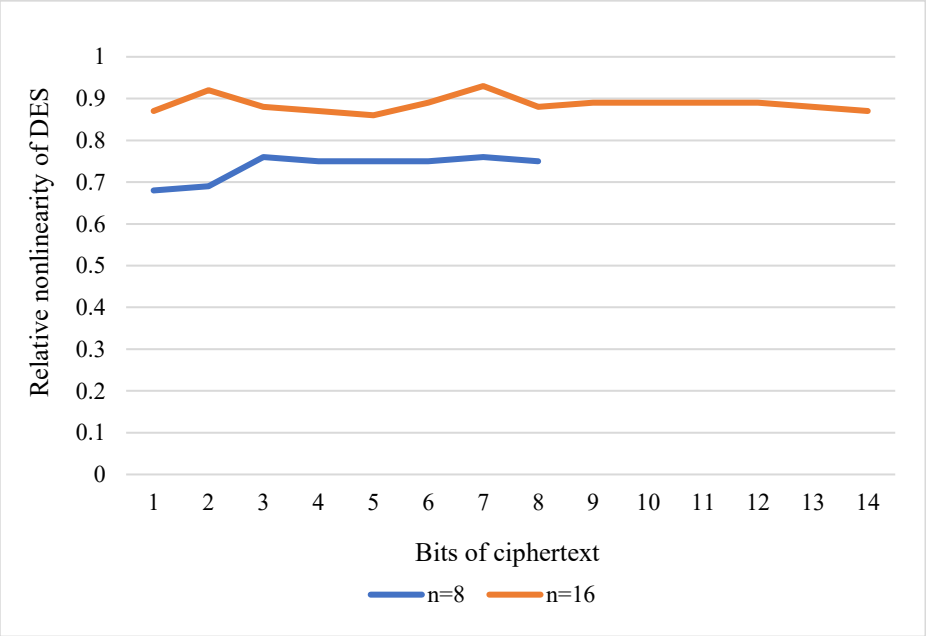

Fig.3 Relative nonlinearity of DES

The results are analyzed as follows:The table shows that the maximum and minimum probabilities in the correlation matrix are close to 0.5, which indicates that the CA used in the tested protocol entity satisfies the avalanche criterion. The relative nonlinearity of each bit of the ciphertext is analyzed for two cases of DES ciphertext grouping block lengths of n=8 and n=16, respectively, as shown in Figure 3.

From the graph of test results, we can see that the distribution of the maximum correlation coefficient of plaintext and ciphertext of DES is between -0.03 and 0.03. In general, the correlation between plaintext and ciphertext is not strong, and it is more difficult to get the relevant information of plaintext from ciphertext, and the algorithm is more confusing to plaintext. As n increases, the relative nonlinearity of DES packet cipher will increase, and the stronger the resistance to linear attacks. The experimental results show that the test scheme proposed in this paper is feasible.

5 Conclusions

In this paper, the study of NSP TT for WCSs introduces the development of wireless communication networks, analyzes the characteristics and security threats of wireless communication networks, and introduces the classical security framework of wireless communication networks on this basis, and then analyzes the NSP TT. However, due to the limited time and ability, the work of this paper in wireless communication NSP testing is not perfect, and the testing of wireless communication NSPs and cryptographic testing schemes need to be further improved to achieve the integration of the two, so that the security protocol testing of wireless communication networks will be more comprehensive and complete.

References

[1] Johannis W, Bietenbeck A, Malchau G, et al. Point-of-care testing (POCT) and IT security concepts[J]. Journal of Laboratory Medicine, 2020, 44(2):107-111.

[2] Putra E G R, Susilo V Y, Mahendra I, et al. Radioiodination of Modified Porous Silica Nanoparticles as a Potential Candidate of Iodine-131 Drugs Vehicle[J]. ACS Omega, 2022, 7(16):13494-13506.

[3] Yu Y, Chen Z, Gan S, et al. SGPFuzzer: A State-Driven Smart Graybox Protocol Fuzzer for Network Protocol Implementations[J]. IEEE Access, 2020, PP(99):1-1.

[4] Haaz E, Thangaraj R, Szori M, et al. Vapor-Liquid Equilibrium Study of the Monochlorobenzene-4,6-Dichloropyrimidine Binary System[J]. ACS Omega, 2022, 7(21):17670-17678.

[5] Higashimoto S, Fujii S, Seike M, et al. Synthesis of Polypyrrole and Its Derivatives as a Liquid Marble Stabilizer via a Solvent-Free Chemical Oxidative Polymerization Protocol[J]. ACS Omega, 2022, 7(15):13010-13021.

[6] Cf A, Yp B, Hs A. Research on non-destructive TT of hydraulic engineering based on improved ALO algorithm and wireless network[J]. Alexandria Engineering Journal, 2021, 60(5):4505-4515.

[7] Kumar A, Panda U, Parihar A, et al. Microfluidics-Based Point-of-Care Testing (POCT) Devices in Dealing with Waves of COVID-19 Pandemic: The Emerging Solution[J]. ACS Applied Bio Materials, 2022, 5(5):2046-2068.

[8] Liu T, Zhang L, Yang D, et al. Evaluation of Uncertainty in Determination of Four Organophosphorus Pesticide Residues in Fresh Tea Leaves by Gas Chromatography[J]. Science and Technology of Food Industry, 2022, 44(1):323-331.

[9] Kovtsur M, Kistruga A, Voroshnin G, et al. Research of authentication failure and ARP injection attacks and methods of their detection in IEEE 802.11 networks[J]. Telecom IT, 2021, 9(1):87-98.

[10] He D, Zhang Y, Li T, et al. Vulnerability Analysis and Security Compliance Testing for Networked Surveillance Cameras[J]. IEEE Network, 2020, PP(99):1-7.

[11] Yan T, Liu J, Niu Q, et al. Network security protection technology for a cloud energy storage network controller[J]. Global Energy Interconnection, 2020, 3(1):85-97.

[12] Dunn A L, Li X . Development of a High-Throughput Kinetics Protocol and Application to an Aza-Michael Reaction[J]. Organic Process Research And Development, 2022, 26(3):795-803.

[13] Yuan L , Chen H , Gong J .Interactive communication with clustering collaboration for wireless powered communication networks:[J].International Journal of Distributed Sensor Networks, 2022, 18(2):261-267.