International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.191-202
http://dx.doi.org/10.14257/ijsia.2016.10.1.18

The Design of WLAN Wireless Access Protocol based on Certified NFC

Jinjin Pan[1,2], YunLi[1,2,3], ZhigangJIN[1,3] and Xunjun Wang[1,2]

[1]*Deparment of Electronic Engineering, Guilin University of Aerospace Technology, Guangxi Guilin 541004*
[2]*Guangxi Experiment Center of Information Science*
[3]*School of Electronic and Information Engineering, Tianjin University, Tianjin 300072, China*
liyun@guat.edu.cn

Abstract

Aiming at the problem of the security of the authentication mode of WLAN wireless access certification, this paper proposes a WLAN wireless access protocol based on NFC certification. The protocol adopts the Diffie-Hellman algorithm established in the unreliable air channel as anonymous AES encryption NFC security tunnel of decryption algorithm, and then using the public key password authentication mode to carries The non anonymous authentication out for the user applying for certification, while determines the conformance certification sides AES key. By shading Petric network modeling, experimental simulation proves that the protocol can effectively resist illegal access to attack and eavesdropping attacks.

Keywords: *WLAN wireless access; NFC certification; Diffie-Hellman algorithm; colored Petric network like to encourage you to list your keywords in this section*

1. Introduction

Wireless Local Area Network, WLAN has a high transmission rate, flexible and other characteristics, and has been applied to university campuses, public places and enterprises. The future with multi-hop function WLAN will become more and more popular in some specific applications, such as wireless, Wireless City Campus etc. However, the open access nature of wireless transmission medium, making WLAN security has become a serious problem. The process of WLAN authentication mainly include WEP, WPA/connected wpa2-psk, WPS three [1-3].However, the weakness of this encryption algorithm is to collect enough IV when RC4 stream of bytes and the first byte, key can be acquired [4]. WPA / wpa2-psk authentication method is widely used, and relatively safe, however, if the users can collect in the certification of 4-way handshake packet when using methods such as dictionary attacks can crack the PSK during the waiting time [5]. On the basis of WPA / WPA2-PSK, the WPS authentication mode is put forward [6].However, this authentication system can not be obtained or rule to judge the legitimacy of PSK users.

To solve the problems above, this paper put forward based on NFC certified WLAN wireless access protocol. NFC (Near Field Communication) is a working frequency of 13.56MHz,working distance is only 0 ~ 20 cm (actually most of the products are less than 10cm) of short-range wireless communications technology that allows electronic devices by simply touching way complete exchange of information and access content and services. NFC technology has been applied to the file transfer, mobile payment, intelligent posters and other fields [7-8]. NFC has three modes of composition, namely card mode, the tag reader mode and ad hoc

ISSN: 1738-9976 IJSIA

mode is used for high-level protocol for communication. This paper proposes a WLAN wireless access protocol based on NFC authentication is developed from the protocol based on point to point mode. However, the point to point mode of NFC also has the problem of eavesdropping in the interaction process. Literature [9] set forth within 10 meters range, NFC data from point to point mode can be tapped. The data is often tampered with the work mode of the point at point NFC is described by literature [10]. Although use a baud rate of 106 active communications can prevent data tampering effectively, however, this approach is very susceptible to middle attacks. Therefore, for the WLAN wireless access protocol and NFC certified safety issues, WLAN wireless access protocol based on NFC authentication uses colored Petri net modeling, with the Diffie-Hellman key exchange algorithm and the second-generation secure hash algorithm to generate near-Based field communication protocol stack secure tunnel. Then, the public key password authentication is adopted, the authentication of the users is non anonymous, and the consistency of the AES key is determined. The simulation proved that: NFC-based authentication for WLAN wireless access protocol running strong enough, you can solve the current wireless LAN attacks and unauthorized access to eavesdropping attacks.

2. WLAN Wireless Access Protocol-Based NFC Certification of Colored Petri Nets

In the practical application, NFC and WLAN respectively, there are many security issues. NFC-based Certified WLAN wireless access protocol is the NFC is the integration of the two mechanisms of NFC and WLAN, and the security of its security is affected by the security of the two mechanisms .So we use colored Petri nets (CPN) analyzes two mechanisms to integrate security issues ,and the improvement is made. NFC-based Certified WLAN wireless access protocol has good protection against illegal access to attack.

As shown in Figure 1, the NFC-based WLAN wireless LAN access protocol CPN model. The model is divided into three regions, namely A region, B region and E region. A region represents a legitimate user behavior (in the NFC Initiator and WLAN in the legitimate user).Area B represents access is available actors (NFC Target and WLAN in the access service provider).Regional E represents the attacker's behavior. In the region E is more fragmented situation, the region E will be broken down into E1, E2, E3, etc. in order to facilitate description. CPN model should be in the same area on the same terminal or device.

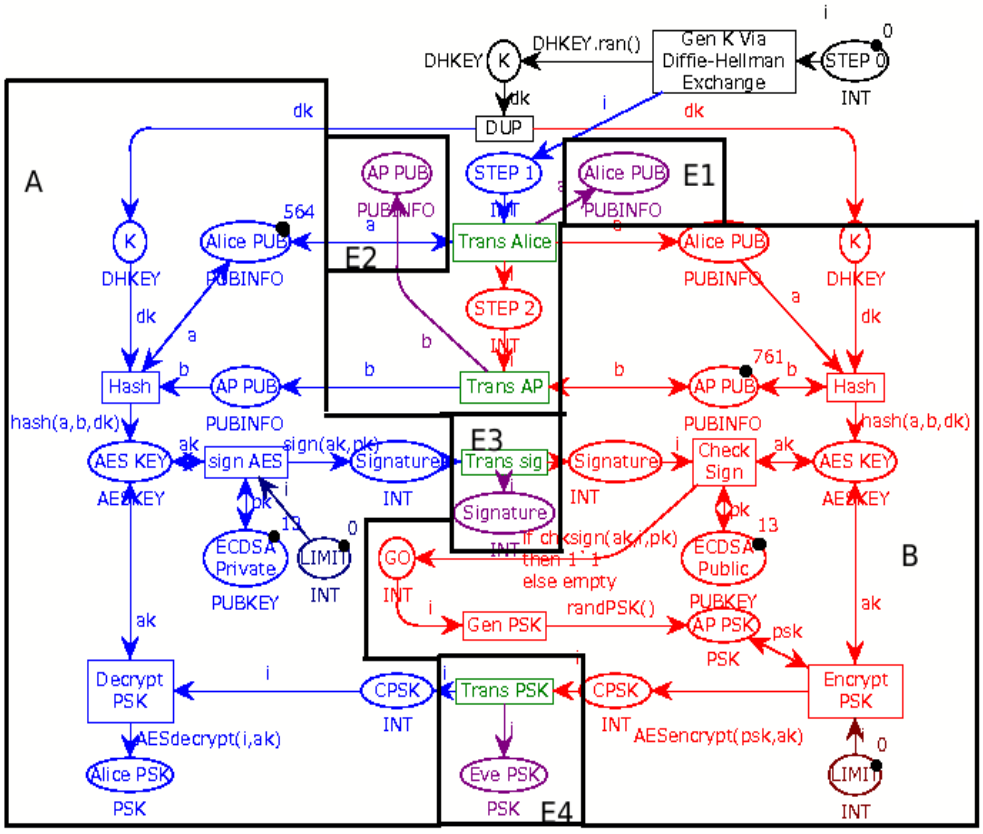

Figure 1. NFC Model based on WLAN CPN Wireless LAN Access Protocol

As enterprises have the following characteristics: turnover is slow, the Internet population is relatively fixed, confidential consciousness is poorer, therefore, for the enterprise user access privileges once initialization is feasible. The Curve Digital Signature Algorithm Elliptic (ECDSA) is used to initialize the public key cryptography system. The user can generate the ECDSA public key for authentication by the software algorithm. The main purpose is to eliminate produce certified public user identity anonymity. After the user's own equipment or using the computer provided by the company to generate ECDSA key pair, you need to be submitted to the spot ECDSA public WLAN administrator to apply for access rights because the process is personally certified by the WLAN administrator, thereby ensuring ECDSA absolute credibility of certificates. Since the protocol uses public key cryptography system certificates, the legal users can enhance the credibility of the applicants by applying the certificate signature to the competent. In this way, the leader signed the electronic signature of the certificate means that the superior agreed the application of the application, which is consistent with the organization's power control mechanism. In this case, the competent leaders signed ECDSA certificate must take full responsibility to review the legality of the applicant.

While the improved NFC protocol can authenticate users, the agreement still needs to establish a secret channel to transmit the configuration information which contains PSK required connect to the WLAN. Diffie-Hellman algorithm can establish secure communications channel in unsafe channels. Diffie-Hellman algorithm, you can establish a secure communication channel in an insecure channel. In order to enhance the resistance to replay attacks, in the process of establishing an encrypted tunnel, the two sides exchanged random information, which occurred in Trans Alice and Trans AP Change. But in this way to establish a

secure channel is anonymous channel, which could not be confirmed to establish the identity of the two sides. Thus, after using the Diffie-Hellman algorithm for establishing a secure channel, the user must authenticate their identity. The security intensity of the Diffie-Hellman algorithm is equivalent to the complexity of solving the discrete logarithm, while the solving of the discrete logarithm is the NP problem. Within the limits of the current level of mathematics and computing ability, the attacker can not quickly solve the oversized discrete logarithm problem. So the secure channel can be guaranteed by Diffie-Hellman algorithm.

Because the Diffie-Hellman algorithm involves a lot of mathematical operations, it is very large to be represented by CPN model, and the Diffie-Hellman algorithm is simplified in Figure 1. Alice and Bob generate K by exchange and calculation process as follows:

First, the Alice is calculated by the formula (1) to generate the A.

$$A = 2^a \bmod p \tag{1}$$

Where in the formula (1), a , p is a large prime number generated randomly by the Alice itself through several Miller-Rabin prime numbers test. After generating a, p, Alice will sent p with a to Bob. Bob, after receiving the p and A, randomly generated a large prime numbers b through several Miller-Rabin prime numbers test, and generate the B by the formula (2). At the same time, the formula (3) is used to generate K.

$$B = 2^b \bmod p \tag{2}$$

$$K = A^b \bmod p \tag{3}$$

At this time, Bob has got K, meanwhile, sent B to Alice .After Alice receiving B, the formula (4) was used to generate K.

$$K = B^a \bmod p \tag{4}$$

At this point, Alice also obtained the same K as Bob's,K is the same the actual value as the K in formula (5).

$$K = 2^{ab} \bmod p \tag{5}$$

After each one respectively to calculate K, Alice as NFC session initiator in a region generates a random INounce. That figure in Alice's pub, through the trans Alice changes sent to area B, the NFC session in the target.

Area B generated random TNounce, after receiving INounce, sent via Trans AP Changes to areas A, at the same time, when the NFCID3 of Target is in close touch through the establishment of NFC session, it has been already transferred from Target to Initiator. TNounce and NFCID3, AP PUB the using libraries in CPN model said, was transformed via the Trans AP changes.

Subsequently, in the Hash changes of the CPN model, Alice and AP uses SHA2-256 algorithm respectively to calculate the KEY with formula (6).

SesKEY is the AES 256 bit symmetric key for AES encryption and decryption algorithm. Because both sides adopted the same algorithm, key, and therefore the two sides calculated is the same, calculating the fundamental elements of K AES 256 - bit symmetric key is generated by their respective Diffie-Hellman algorithm calculation, Eve can't intercept K. And even though the region such as E1 and E2 the CPN model ,Eve can intercept INounce, TNounce and NFCID3 in the time, also because of the lack of K, Eve can not use hash function to calculate the correct AES 256 - bit symmetric KEY, namely the AES KEY of CPN model. After the AES 256 bit symmetric key is obtained, secure channel based on NFC has been successfully established. However, this channel is anonymous. For access request, the further authentication of user's identity is needed, at this time, you can use the ECDSA

certificate described previously. Because the two sides have the same AES 256 bit symmetric key so Alice can use a private key to digitally sign the AES 265 bit symmetric key in the change of the sign AES, and send the signature to area B through Trans SIG changes, after area B receiving the digital signature, using the corresponding public key which is not revoked in database to test the generated AES 256 bit symmetric key. f the verification signature is correct, it is proved that Alice has the corresponding networking authority. Using ECDSA certificate to sign for AES key has four advantages: First NFC protocol is designed to close the low-speed data transmission protocol, AES is calculated on both sides, signature of AES can take advantage of the existing data to reduce a protocol data transmission, and reduce the waiting time for users. Secondly, earlier steps stated has a very low probability because of a computer failure resulting in an inconsistent AES 256 bit symmetric key. The agreement of AES symmetric key can be verified by the verification of public key signature. Third ECDSA public key cryptosystem is safe enough, even if the signature was been eavesdropped in E3 by Eve, it is not enough to reverse crack the AES symmetric key through signature. Fourth, through the verification of AES signature, the middle attack can be averted. This solves the problem of the NFC eavesdropping and the middle attack.

If the signature verification fails, it means that AES symmetric key is inconsistent or user's identity is illegal. Region B can end authentication session. Based on the successful signature verification, the regional B can precede the next step process.

At this point, AP needs to use some kind of complex algorithms, whose entropy is high enough, such as reading from / dev / urandom device under Linux in a string of random length of more than 16, including PSK case letters, numbers, special characters, and randomly generates a ESSID. After the configuration information passed through AES key encryption and sent to the area A by Trans PSK Changes. Because the configuration information has been encrypted by AES and even as the Eve intercepted the encrypted data in Region E4, it still can not be solved within a valid time PSK without getting the AES key. In this way, the confidentiality of PSK transmission is realized. After receiving the encrypted configuration information, the area A can use the AES key to decrypt the configuration information, and finally get the random PSK and random ESSID generated by AP. Because in each authentication of NFC, the Gen PSK changes in area A will generate new ESSID and PSK, t will also be useless even Eve stole the decrypted PSK from Alice because for the WLAN access protocol of NFC authentication, ESSID and PSK for each WLAN connections are different. This would solve the problem of channel isolation and user security in wireless LAN communication.

As shown in Figure 2, the simulation results indicate that, in the entire authentication process, the Eve can intercept the INounce transmitted by the area A in area E1, and intercept the TNounce and NFCID3 in the area B by the area E2. However, because the K can not be got from the Diffie-Hellman exchange, it can't calculate the AES symmetric key. Subsequently, Eve intercepted the signature of Alice to AES symmetric key in the area E3, but the signature obtained is meaningless. After the changes of Encrypt PSK, Eve intercepted the encrypted configuration information of PSK and ESSID in the area E4.However, under the condition of no AES symmetric key, the Eve can't decrypt the information in PSK Eve completely. After area A decrypted the encrypted information, finally in the Alice PSK libraries have the same configuration with AP PSK library information,but eavesdropping information in Eve PSK library is different from AP PSK library. Ultimately, Bob completed the secret transmission of PSK successfully .In the check sign changes, Bob has also completed the confirmation of the identity of Alice, the authentication of Eve will be rejected, because there is no public key in the Public ECDSA library. After solving the problems of anonymous authentication,

user compromised, channel segregation, we will solve the problems of WLAN illegal access and wiretaps.

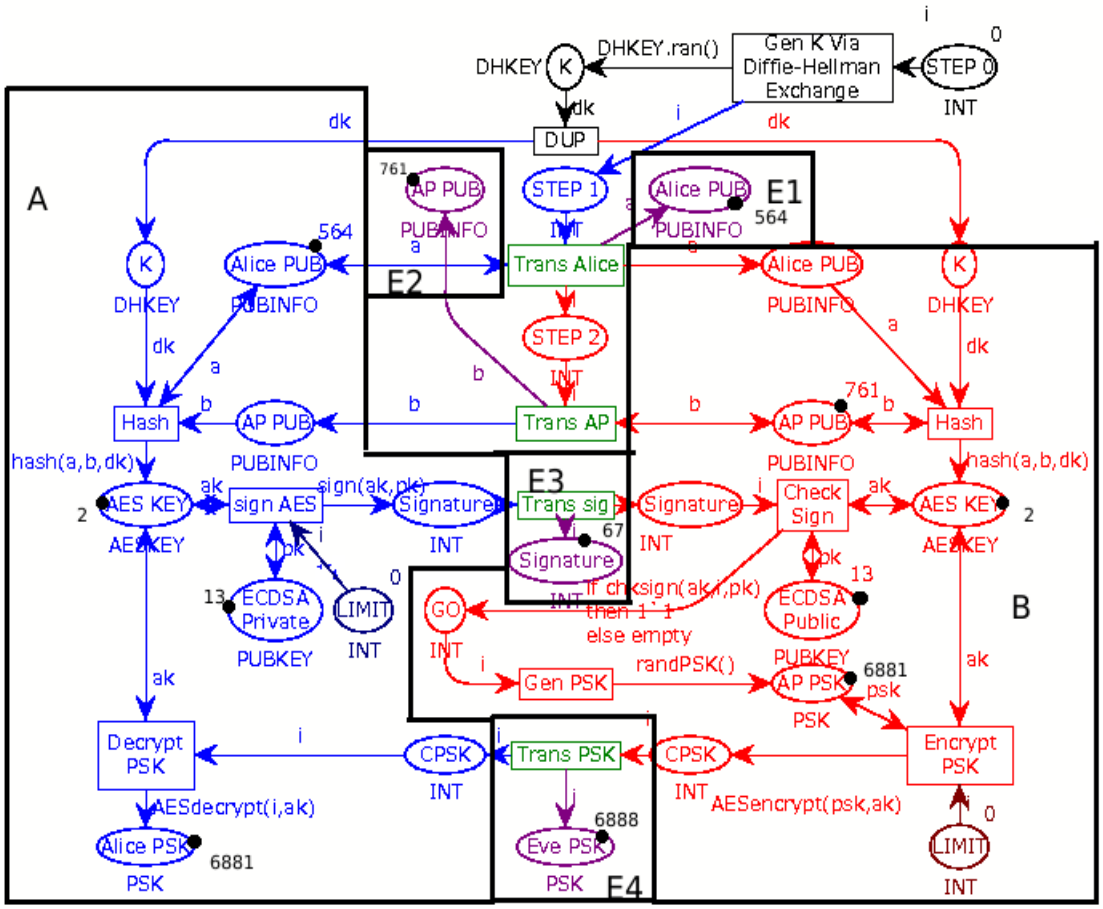

Figure 2. CPN Simulation Results of the WLAN Access Protocol via NFC authentication

3. Design of WLAN Wireless Access Protocol based on NFC Authentication

3.1 time sequence diagram of WLAN wireless access protocol based on NFC

Figure 3 is a timing diagram of the WLAN access protocol based on the NFC authentication. STA represents the user's WLAN equipment, as in the NFC initiator role, and in Alice's position in cryptography, e user's NFC device is represented by the Initiator / Alice. STA and Initiator / Alice are on the same device.

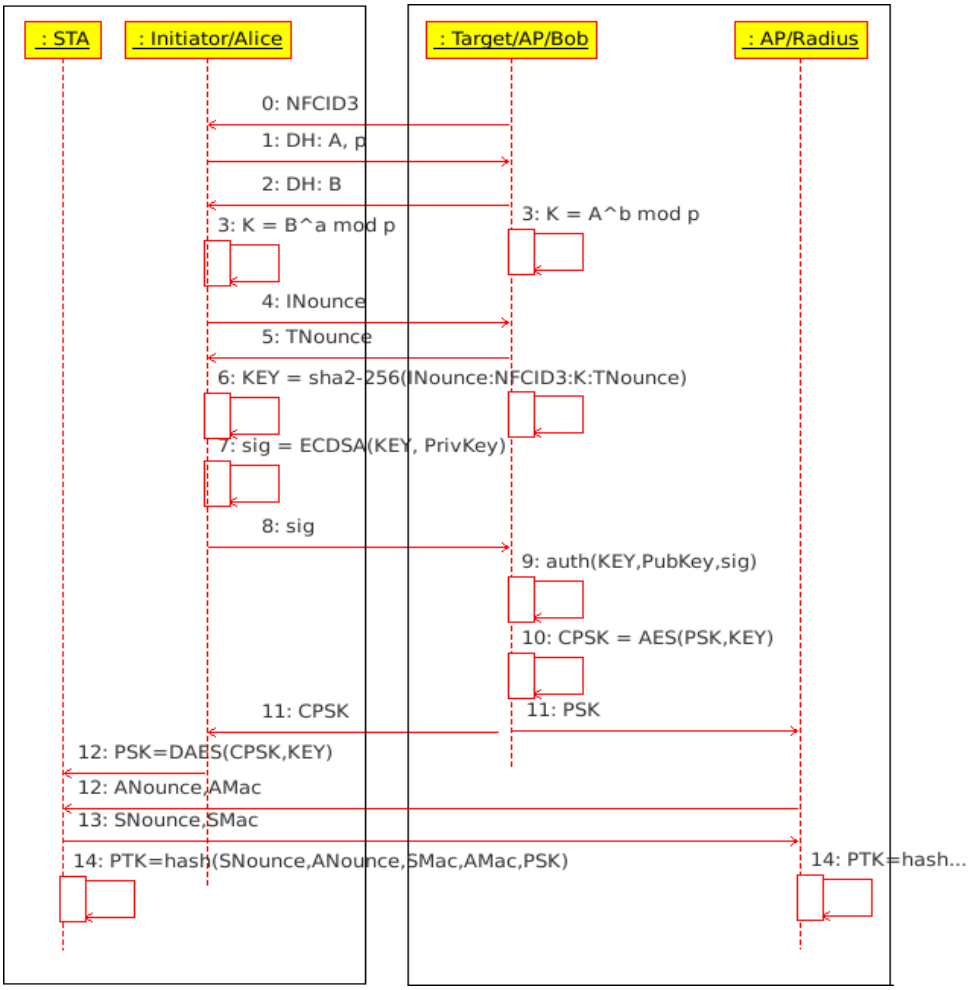

Figure 3. WLAN Access Protocol based on NFC

The corresponding NFC devices which receives the request of WLAN access authentication is in the NFC Target role, that is, the Bob role in cryptography, this device bind with AP on a device generally. Thus, in the sequence diagram it is named Target / AP / Bob. And the device accepted the STA in WLAN connection generally called AP, the authentication part is sometimes referred to the Radius server. Of course, under normal circumstances, they are bound together. So named AP / Radius. Minimum requirements for Target / AP / Bob and AP / Radius is in the same area that will not leak, so you can ensure the server supporting NFC authentication will not leak during the communication with the AP.

Time flow of sequence diagram is from top to down, it can be considered as co-terminal device inside the same large frame, and without breach it can be considered that there is no leakage incident, nor can it be tapped. And the arrow across the border is the protocol of the air communications, this communication striding across the terminal can be tapped through a special antenna. So the security of air communication must be guaranteed by protocol encryption.

In general, the WLAN access protocol passed the NFC certification has 15 steps protocol operation from the NFC access to the final PTK. The 15 steps are:

(0) User holds the device as Initiator role to establish a NFC session with Target the authenticator, in the process, Target will send NFCID3 to Initiator.

(1) Initiator generated a, p randomly, calculated A according to formula (1),and sends the a, p to Target.

(2) Target generated b randomly, calculated B according to formula (2), and sends B to Initiator.

(3) Target and Initiator are separately generated K by the calculation of the formula (4)

(4) Initiator randomly generates INounce and sends it to Target.

(5) Target randomly generates TNounce and sends it to Initiator.

(6) Target and Initiator individually generates 256 bit symmetric key KEY for AES encryption respectively according to the formula (6)

(7) Initiator uses its own private key PrivKey to sign KEY, generating the signature SIG

(8) Initiator sends SIG to Target.

(9) Target use the PubKey stored when user is applied for the Internet in advance, and verify the signature of KEY. If you pass, Target generates the configuration information containing the random PSK and random ESSID, denoted as PSK.

(10) Target uses KEY to encrypt PSK generated in the ninth step containing the configuration information in AES, generates encrypted data CPSK.

(11) Target sends CPSK to Initiator, configures the AP/Radius with the configuration information defined by PSK at the same time, and gets ready for access to the user.

(12) Initiator will use the KEY to decrypt CPSK in AES, transmit the obtained PSK to the WLAN networking module STA. Meanwhile, AP / Radius completed the configuration, and successfully sent ANounce with AMac to STA.

(13) the STA accepts the first WPA/WPA2-PSK handshake launched by AP / Radius,sends SNounce and SMac.

(14) STA and AP/Radius respectively uses SNouce, SMac, ANouce, AMac, as well as PSK with ESSID and PSK to generate PTK in accordance with the WPA protocol standards, and complete follow-up of the third and fourth handshake. So far, WLAN access protocol had been all completed through authentication of NFC.

Through the steps above, you can transfer the PSK on the basis of no plaintext to accomplish the security access of WLAN. And because the PSK using Diffie-Hellman has generated the NFC security channel which is difficult to break through the transmission process. Eavesdropping almost impossible to PSK crack at the effective time.

4. Simulation

In order to verify the effectiveness of NFC-based certified WLAN wireless access protocol, the paper mainly emulates from two aspects: defense simulation of illegal access attack to verify the protocol can effectively prevent illegal access attack; defense simulation of eavesdropping attacks to verify that the protocol proposed can effectively prevent eavesdropping.

As shown in Figure 4. The actual simulation process shows that the Eve is likely to certificate the PSK data which is sent to Alice before Alice. If the agreement is only authenticates the user and NFC secure channel is not built by Diffie-Hellman algorithm in the previous stage, and use the NFC security channel to transmit the configuration information, Eve is entirely possible to eavesdrop configuration information in a plain text after Alice's public key was authenticated, and complete illegal access before Alice. So it is necessary to transfer PSK and other configuration information through the establishment of NFC secure channel. If Eve didn’t complete illegal access before Alice, then 0 the representative of Eve also can not enter the state Auth Pass, but was suspended in Air base after Send Auth change, and can not enter the Fail library. This suggests that, after Alice was certified, ach time a password has caused the failure of the authentication password. Eve is unable to carry out the second certification, which shows that a password authentication is

necessary for preventing replay attack. Despite the Eve intercept a large amount of data, but due to the lack of K, the AES symmetric key is still can be calculated, then it is impossible for encrypted CPSK to decrypt, eventually it was rejected in the Auth changes because of the wrong configuration information. Entered the Fail state. And because legitimate users Alice can decrypt the PSK configuration information correctly, then entered Auth Pass status successfully. It can be seen that the WLAN access protocol is effective for resistance of the illegal access attacks through NFC authentication.

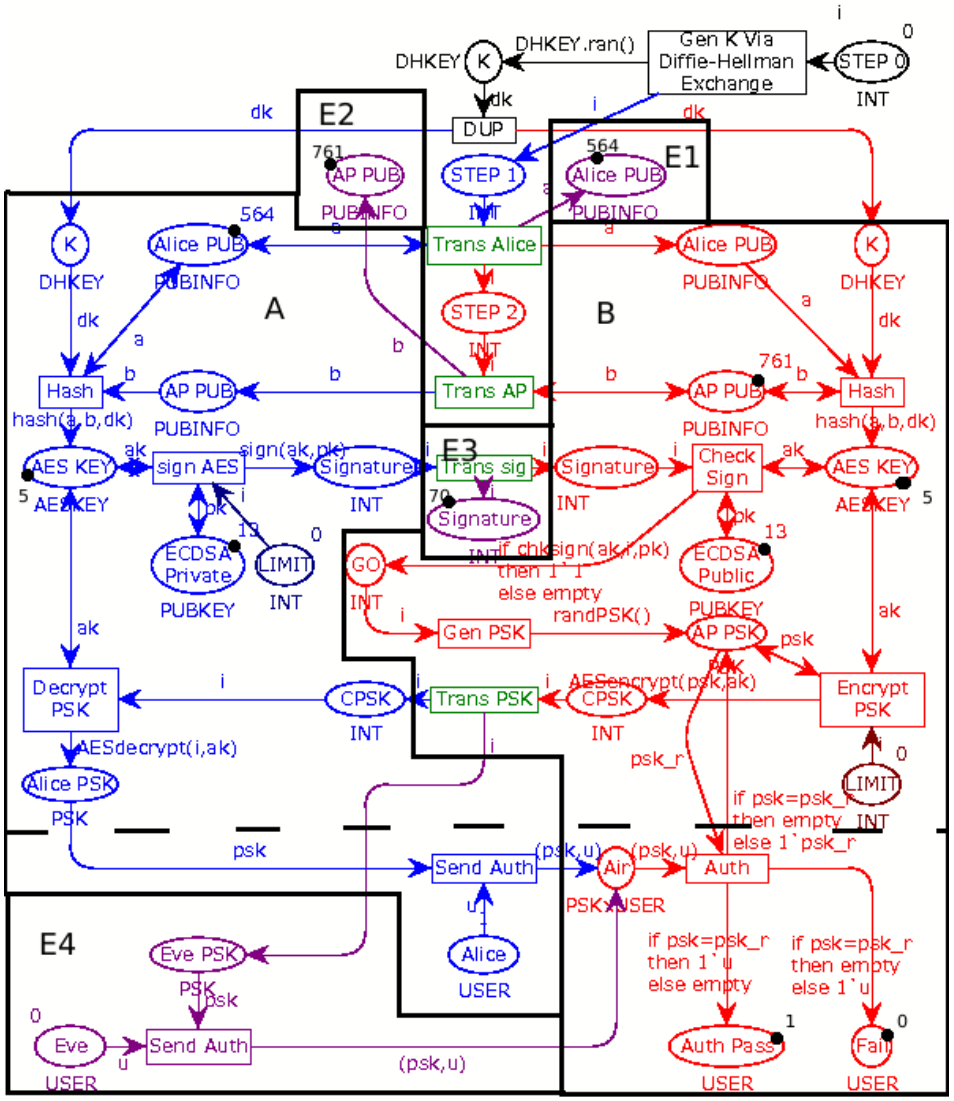

Figure4. The Results of the CPN Simulation of the Resistance for Unauthorized Access through WLAN Access Protocol Authenticated by NFC

As shown in Figure 5, the area A and the area B encrypted the transmission of WLAN access configuration information generated randomly. In this process, Eve has eavesdropped NFC exchange data in area E1, E2, E3,but those eavesdropping exchange data can be used to calculate AES symmetric key, and it can only intercept encrypted configuration information in Trans PSK change, ut is unable to decrypt the configuration information. After Alice PSK Library obtained the decrypted configuration information in

area A, area A and area B calculates the consistent PTK respectively through the to PTK change. Then the Data Send Library in the area A will use the PTK to encrypt, and the area B will also use the PTK to decrypt anf put it into the Data Recv library. Since the two PTK is consistent, the final data in Data Recv will be the same as the original Data Send. due to the lacking of PSK in area E4,Eve intercept SNounce, anounce, SMac, AMa the public information of area A and area B exchange from air through Trans A and Trans S two vicissitudes . But it unable to generate correct PTK. Eve also intercepted PTK encrypted data in area A during TD change, but because the PTK in area E4 is different from the PTK in area A after decryption of the vicissitudes of the Eavesdropping in area E4, Data Eaves library can only get the wrong decrypted data, from Figure 5 it can be seen that data in Data Eaves is different from the data in Data Recv. This shows that the WLAN access protocol passed through NFC certification is effective for the resistance of eavesdropping attacks.

At the same time, since each certification will generate new random ESSID and PSK configuration to ensure the property of each time a password. Because the different users can not know the configuration information of others, the attacker can not rely on their own PSK to calculate the PSK of other people, so that the user channel is isolated. This is the same principle as that the Eve is unable to tap the area A in Figure 5 and the communication of the area B. Because different users get different PSK, causing them to calculate the different PSK with the other information under the same conditions, thus, it can resist the eavesdropping attack based on the same PSK of inside man.

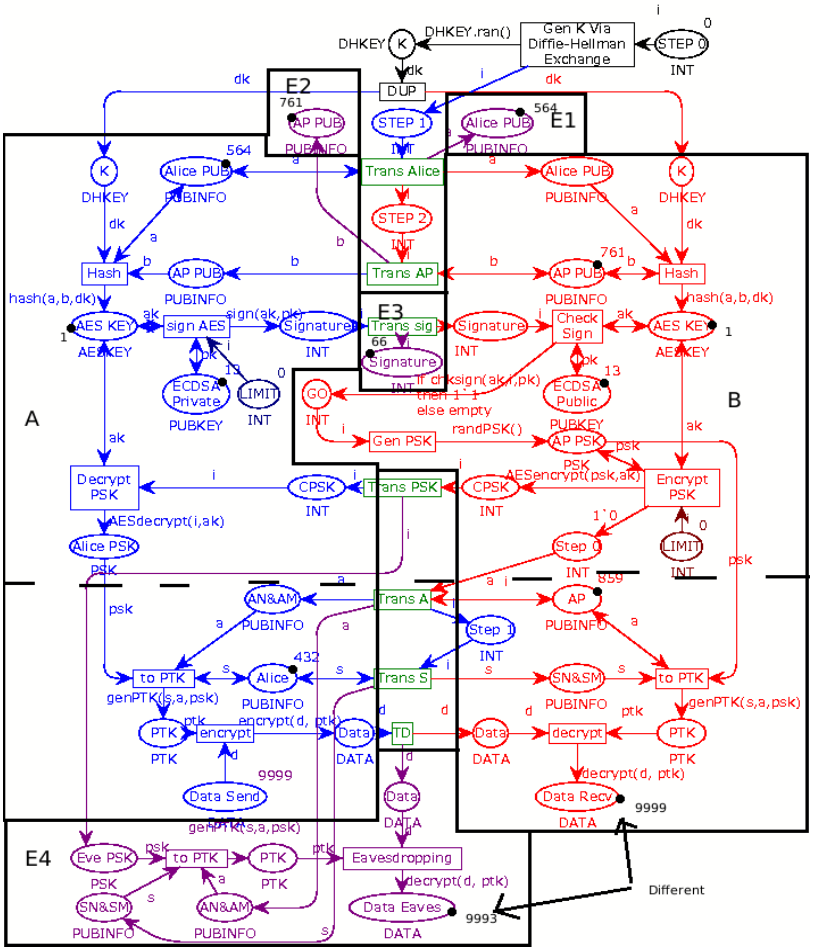

Figure 5. CPN Simulation Results of the WLAN Access Protocol based on NFC Authentication for Eavesdropping

5. Summary

In order to solve the security problem in the authentication process of WLAN, the WLAN wireless access protocol based on NFC is proposed in this paper. The protocol uses Diffie- Hellman algorithm in the unreliable air channel established anonymous NFC security tunnel using AES as the encryption and decryption algorithm. Then, the public key password authentication is adopted to carry out the non anonymous authentication for the users applying for certification. And the consistency of the AES key on both side is determined. The protocol was validated by the colored Petri net that it can effectively resist illegal access attacks and Eavesdropping attacks, and has good stability.

Acknowledgments

This work was supported in part by open foundation of Guangxi Experiment Center of Information Science LD15030X, research fund of Guilin university of Aerospace technology YJ1403，Guangxi science and technology development project 1598008-29, Guangxi university of science and technology research projects ZD2014146，GuangXi District natural science fund 2015GXNSFAA139298.

References

[1] Xu L; He W; Li S. Internet of Things in industries: A survey[J]. Industrial Informatics, IEEE Transactions on,vol. 10, no. 4, **(2014)**, pp. 2233-2243.
[2] Atzori L; Iera A; Morabito G. The internet of things: A survey[J]. Computer networks, vol. 54, no.15, **(2010)**, pp. 2787-2805.
[3] Coskun V; Ozdenizci B; Ok K. A Survey on Near Field Communication (NFC) Technology[J]. Wireless personal communications,, vol. 71, no. 3, **(2013)**, pp. 2259-2294.
[4] Sheldon F T; Weber J M; Yoo S M, et al. The insecurity of wireless networks[J]. Security & Privacy, IEEE,, vol. 10, no. 4, **(2012)**, pp. 54-61.
[5] Mukherjee A; Fakoorian S; Huang J; et al. Principles of physical layer security in multiuser wireless networks: A survey[J]. Communications Surveys & Tutorials, IEEE, , vol. 16, no. (3), **(2014)**, pp. 1550-1573.
[6] Marco D A; Giorgio C; Antonio L. Dependability in Wireless Networks, Can We Rely on WiFi?[J]. IEEE Security & Privacy, vol. 5, no. 1,**(2007)**, pp. 23-29.
[7] [Park K Y; Kim Y S; Kim J. Security enhanced IEEE 802.1 x authentication method for WLAN mobile router[C]. Advanced Communication Technology (ICACT), 2012 14th International Conference on. IEEE, **(2012)**, pp. 549-553.
[8] Hwang H; Jung G; Sohn K; et al. A study on mitm (man in the middle) vulnerability in wireless network using 802.1 x and eap[C]. Information Science and Security, 2008. ICISS. International Conference on. IEEE, **(2008)**: pp. 164-170.
[9] Y. Zhe, "Wireless network security offensive and defensive combat. [M]", Beijing：Publishing House of Electronics Industry, **(2011)**.
[10] Wi-Fi Alliance. Wi-Fi Protected Setup Specification Version 1.0 [S]. **(2007)**.

Author

Jinjin Pan was born in Guilin, Guangxi Province, in 1971. She is now an associate professor and currently working in Guilin University of Aerospace Technology as a teacher. She majors in communication and network.