Charging wireless sensor network security technology based on encryption algorithms and dynamic model

Yuanming Li¹,², Wei Guo¹,², Xuejun Meng¹,² and Wen Xia¹,²

Abstract
With the popularization of the Internet, the related information technology is developing faster and faster, and the scale and complexity of the network are also increasing. Wireless networks cover all aspects of life, along with it, network security issues have gradually emerged. In recent years, network security vulnerabilities have been exposed continuously, from WiFi to Bluetooth, people gradually realize the security of wireless networks. The purpose of this article is to solve the existing security problems and study the operation process of RC4 and Advanced Encryption Standard algorithms, and the improvement scheme is put forward. This article is based on the inherent media access control address filtering technology of wireless network card; a dynamic security model for wireless networks is proposed and constructed. Devices accessing the network use 802.1x authentication method and distribute and set security status values for each device, the authentication server uses Remote Authentication Dial in User Service. This article uses the method of virtual private network encryption network to provide an encryption layer for communication between devices and wireless networks, thus, the data in network transmission can be encrypted and protected. In this article, the structure and strategy of Remote Authentication Dial in User Service are changed, in order to ensure the high security of wireless network equipment in the connection process. In the testing phase of this article, we have tested the model in detail several times. Tests are divided into middleman and session interception tests. A large number of test results show that this model can improve the security of wireless network and has good performance.

Keywords
Wireless network, encryption algorithm, dynamic security model, network security

Date received: 17 November 2019; accepted: 17 December 2019
Handling Editor: Mohamed Elhoseny

Introduction
Since the popularity of wireless networks, because of its obvious mobility advantages over wired networks, it has also driven the development of many of our mobile devices. In some public places such as hotels, shopping malls, and so on, wireless hotspot coverage has been greatly improved.¹-⁴ Regarding our daily life, all aspects of food, clothing, housing, and transportation have network applications, such as: Taobao, Meituan, hungry, all kinds of taxis, office automation systems are inseparable from network development, the development of computer networks has promoted the times. An individual involved in development has profoundly

¹State Key Lab of Astronautic Dynamics, Xi’an, Shaanxi, China
²China Xi’an Satellite Control Center, Xi’an, Shaanxi, China

Corresponding author:
Yuanming Li, State Key Lab of Astronautic Dynamics, Xi’an 710043, Shaanxi, China.
Email: 20131102@xpu.edu.cn
realized the power of change in the information age. People’s lives are now spread in large and small networks. At present, the rapid development of wireless networks has broken through the constraints of wired network physical hardware, enabling the network to access anytime, anywhere, and accessing the Internet anytime, anywhere. The superiority plays an important role in the use of network applications and mobile portable devices. Nowadays, a large number of wireless network users in China only stay on the basis of use, and have no security awareness for network security. Compared with wired networks, most of the wireless networks are deployed by users through wireless routers and portable WiFi devices. The user’s security awareness is insufficient. In order to save capital investment, the importance of security devices such as firewalls to wireless networks is ignored. It is bound to cause the very low security of small and medium-sized wireless networks.

In response to the problem of wireless networks in the past, Institute of Electrical and Electronics Engineers (IEEE) has advocated some prevention methods, which are divided into three network security services. The first is to verify access to the wireless network access client, to ensure that it is a legitimate device to access the network. The second is to encrypt the connection information to avoid leakage of private information. The third is to require integrity in the process of information transmission. Of the three security services mentioned above, the first two services are more involved. The wired equivalent privacy (WEP) agreement appeared in 1997. On this basis, after some improvement, WEP2 appeared. Since the development of WiFi, there has also been a security protocol Wi-Fi protected access (WPA) for WiFi. Today, the most used encryption protocol is the Extended Encryption Standard (AES) encryption standard. The development of various encryption protocols is especially important to protect data security.

Protection technologies for wireless network security are constantly evolving and are currently divided into two phases. The first encryption protocol is WEP, which uses a static key that is 64 bits in length. Its encryption algorithm uses RC4. In the research of RC4, Miyaji and other scholars have studied the new linear correlation, including the unknown internal state variables in general RC4 and WPA. From their experiments, they successfully discovered various new linear correlations and theoretically proved some correlations. In order to solve several problems in the first generation of security protection technology, WEP2, the message integrity check mechanism Temporal Key Integrity Protocol (TKIP), and AES came into being. In response to the weaknesses and shortcomings of the previous generation of WEP, Kai Jun and other scholars gave an introduction and introduced a new generation of wireless network security standard 802.11i. For the process of TKIP and CCMP encryption, they have proved through experiments that CCMP encryption is more secure. For WPA-Enterprise (PEAP) networks, ROBYNS and other scholars have discovered some security risks. You can use a class of vulnerable devices as a springboard on which to use a malicious access point to capture Lightweight EAP (LEAP) MSCHApv1 credentials and convert them to PEAP MSCHApv2 credentials, stealing credentials for network connections, and then illegally connecting Internet.

This article studies and analyzes the operation process of RC4 algorithm and AES algorithm, and proposes and constructs a dynamic security model of wireless network. Borrow media access control (MAC) filtering technology and use improved detection methods. The authentication server uses Remote Authentication Dial in User Service (RADIUS). This article uses the virtual private network (VPN) encryption network method to provide an encryption layer for communication between the device and the wireless network, so as to be able to encrypt and protect the data in the network transmission. This article changes the structure and policy of RADIUS to ensure the high security of wireless network devices in the connection process.

Proposed method

Today, the IEEE 802.11b standard is still being applied, especially the WEP security protocol, which has serious security problems. WEP mainly uses the RC4 encryption algorithm. The following article will analyze the RC4 encryption algorithm and the AES algorithm in detail.

RC4 algorithm

The RC4 algorithm is an algorithm developed by Ron Revest in 1987. When it first came out, it had some good advantages, such as anti-analytical ability, and then promoted quickly. The composition of the RC4 algorithm consists of two parts. The first part is called Key Scheduling Algorithm (KSA). By arranging a key $K$ (usually $K$ length 64/128 bit) of $L$ (representing the length of the key $K$) byte, an arrangement $S[0, 1, 2, ..., N' - 1]$ is generated, $N'$ is generally 256; The second part is the Pseudo Random Generation Algorithm (PRGA). The pseudo-random key sequence $Z[i]$ is obtained by PRGA. The encryption or decryption function can be implemented separately by differentiating the key sequence with $P[i]$ or $C[i]$ or generating a ciphertext.
**Improvement of RC4 algorithm representation method**

**Improved initialization of the RC4 algorithm.** From the research of the existing RC4 attack method, it is found that many attacks on the RC4 algorithm are directed to the initial state $S_0$ in the PRGA, and finally all the correct key bytes are recovered. In the PRGA operation process, the state $S$ before and after the byte output is basically unchanged, and the attacker mainly concentrates on the PRGA stage. The improvement of this algorithm is to protect information security by exchanging bytes and adding algorithm complexity.

Step 1: Perform the original algorithm step operation;
Step 2: Exchanging $S[i_m]$, $S[j_m]$, and performing the operation after the exchange, the position byte of $S[i_m]$ is $X[t_m]Y[t_m]$ ($t_m = 1 - F$). The position byte of $S[j_m]$ is $X[n_m]Y[n_m]$ ($n_m = 1 - F$), and the position of the line is shifted right, and the moving distance is $|X[n_m] - X[t_m]|$, so that $S[t_m]$ is in the same column as $j_m$, and then moves the column where the position is located downward. The moving distance is $|Y[n_m] - Y[t_m]|$, so that $S[t_m]$ reaches the position specified by $j_m$. By such a transformation method, the position $S[j_m]$ where $j_m$ is located is shifted, and the distance of the right movement is $(16 - |X[n_m] - X[t_m]|)$, and the displacement distance under the column is $(16 - |Y[n_m] - Y[t_m]|)$, so that $S[t_m]$ reaches the position of $S[j_m]$;
Step 3: Perform the original algorithm step operation and output the key byte.

**RC4 algorithm penetration test.** WEP uses the RC4 algorithm for encryption. In the WEP application, the RC4 algorithm combines a changed initial vector (herein-after referred to as "IV") and the shared key to form a key, and then undergoes the KSA algorithm operation, and then the PRGA operation, and the result output by the PRGA is then combined with the plaintext. Perform an exclusive OR operation and finally output the ciphertext.

In the KSA, the Scrambling cycle performs the state of $S$ after $i$ cycles, which is denoted as $S_i$, where $i = -1, 0, 1, 2, \ldots, N - 1$, $S_{-1}$ indicates before the first cycle. Arrange the state of $S$, then, for a certain $i$, assume $X = S_i[1]$, $Y = S_i[S_i[1]]$, $Z = S_i[1] + S_i[S_i[1]] = S_i[X + Y]$ as shown below.

### 1. Using the first byte to attack

Considering Swap in KSA as random, we know that the probability of $X$, $Y$, and $Z$ appearing after $i$ cycles is only 5%. In WLAN, it is not difficult to get the first output of PRGA. In general, the first field in the plaintext is the icon of the TCP/IP protocol, and the first output byte of the PRGA can be obtained by XORing the byte with the intercepted ciphertext. It can be proved that the 5% probability that occurs after $i$ cycles makes

$$Z[1] = S_{i+3}[A + 3]$$  \hspace{1cm} (1)

where

$$S_{i+3}[A + 3] = S_{i+2}[j_A + 3]$$  \hspace{1cm} (2)

Numbers of $Z[1]$ in $S_{i+2}$ can be searched by computer to compute $j_A + 3$. Because

$$j_A + 3 = j_A + 2 + S_{i+2}[j_A + 3] + K[A + 3]$$  \hspace{1cm} (3)

Then an estimate of $j_A + 3 - j_A + 2 - S_{i+2}[j_A + 3]$ can be obtained. When the $X$ values are different, a plurality of different estimates can be obtained, and the number of occurrences is also different. The most frequently occurring value is selected from all the estimates as the final estimate of $K[A + 3]$. By repeating the above process, the values of $K[A + 4]$ and $K[A + 5]$ can be found one by one, and finally all the keys SK are obtained. The above is called "special condition first byte attack," this is referred to as method 1.

By the above method, it can be concluded that the more general conditions for using the IV Weakness attack are

$$S_{i+3}[1] = X \equiv A + 3$$  \hspace{1cm} (4)

$$X + S_{i+3}[X] = A + 3$$  \hspace{1cm} (5)

Using this formula, IVs can be calculated for analysis. A similar attack experiment is performed on the required IV, which is called "general condition first byte attack," and this is called method 2.

### 1. Using the second byte to attack

In WEP, $K[0]$, $K[1]$, and $K[2]$ are known IVs, and we hope to obtain $K[3]$, $K[4]$, ... To obtain the value of $K[3]$, a special IV format $(3, N - 1, x)$ must be constructed, and $x$ can take values without affecting the result.

In state $S_1$, let $X = S_3[1] = 0, Y = S_3[X] = S_3[0] = 3, Z = S_3[X + Y] = S_3[3]$, then you can get $X$, the probability that none of the three elements of $Y$ and $Z$ participate in any one of the KSAs is 5%. Because

$$S_3[3] = S_3[j_3] = Z$$  \hspace{1cm} (6)

The researcher retrieves a value of $Z$ according to $S_2$, and obtains the position subscript $j_3$ of the item, and according to
used to obtain the key, the above method can also be applied to the above method, and the value with the highest frequency of occurrence may be \( K[3] \) value.

When the second output byte analysis method is used to obtain the key, the above method can also be utilized, but the condition to be satisfied becomes

\[
S'_{d+3}[2] + S'_{d+3}[1] + S'_{d+3}[2] = A + 3
\]

The first formula in the condition is the basic condition of the attack analysis. The significance of the second and third formulas is to prevent the unknown uncertain elements from participating in the exchange in the second cycle of the PRGA.

Among the above conditional expressions, only \( S_{d+3} \) specifically meets the requirements, and only after it is converted can it be used for actual attacks. Here, using the computer search mode, applying the induction method to the IV, the condition for obtaining the key including the IV can be obtained.

**Principle of AES encryption algorithm**

The design requirements of the AES algorithm are packet encryption, which is easy to generalize and easy to use for hardware and software production. There are several encryption techniques to implement permutation and replacement during AES operations. The AES algorithm has four key operations: KeyExpansion, AddRoundKey, Nr-IRound, and FinalRound.

In the AES algorithm, each key of the packet encryption should have the participation of the extended key Expandedkey(\( i \)). The specific process is as follows:

Circle transformation. Each transformation consists of the following three layers:

1. Nonlinear layer—Perform Subbytes. The byte conversion can be mapped by the calculated S-box, so Subbytes is also called S-box transformation, which is a process of byte substitution.
2. Linear mixed layer. Perform ShiftRows transformation (row displacement transformation). Sequence shifting is performed in the ShiftRows transform; MixColumns, also called column confusion, treats each column in the state as the result of multiplying a \( X \) and \( C(X) \) on GF \( (2^8) \). ShiftRow transform is to shift the row in the state, specifically determined by the value of \( Nb \), in the key plus layer—perform AddRoundkey (round key addition) operation.
3. Output layer, output according to the operation results of the previous two layers.

**Disadvantages of existing network security models**

For the P2DR2 model, even if it is used very frequently, it has a certain protective effect. However, with the rapid development of the Internet around the world, it has slowly revealed a series of shortcomings, mostly,

1. The P2DR2 model does not involve a secure active reporting mechanism. At each stage of the model, it is directed to the abnormal situation in the model, and the monitoring of the attack behavior by the suspected attacker, which will form many log records stored in the hard disk. For these logs, the administrator needs to look it up, and it does not actively push exceptions and logs to the administrator. This will cause a delay in the alarm condition. If the model can actively push all the abnormal conditions and security logs to the security administrator, and also give the administrator some corresponding improvement suggestions, the system repair speed and administrator workload can be optimized. Because the log content is very complicated, not easy to read, and the report module is missing, if the report module is added, the whole system can be made more efficient and stable.

2. The network security risk analysis function is weak. In this model, the risks that the network may face are not analyzed. Traditional networks are only subject to relatively single security threats, and there are various threats in the network, including virus propagation and hacking. Therefore, if the programmers program each possible situation and summarize a set of special solutions to realize the intelligent analysis of risk analysis, it will inevitably greatly enhance the security and stability of the entire system, and also make the work more efficient.

3. There is no function related to early warning in the P2DR2 model. It is important that the early warning function can actively analyze the current security risks in the network and proactively remind the administrator to prepare for this. Early warning functions may require a higher intelligence algorithm to achieve. This requires the continuous development of artificial intelligence. In the initial stage, the
vulnerability scanning tool can be used to implement the analysis, and the result of the analysis is determined by the algorithm intelligent corresponding solution, so that the result is actively pushed to the administrator, and the administrator can take countermeasures.

For today’s security model, a large part of the research only stays on encryption and authentication technologies, and there are very few studies on dynamic detection and protection. Static can only meet the protection needs of network security in the early stage of wireless network, and cannot meet the current security situation. So for today’s network situation, the existing security model is not perfect.

Construction of wireless dynamic security model

The shortcomings of the existing models are briefly analyzed above. In response to the above drawbacks, an improved security model will be constructed below.

The facts show that static models cannot meet existing needs. The dynamic security model designed in this article is based on 802.1x technology and VPN encrypted data transmission method, designed and developed for wireless network security features.

The main process of the dynamic model designed in this article is based on MAC address binding and IP address binding, and a pioneering addition of an identifier (SSID). When the user equipment is connected to the network, not only the above two addresses will be bound, but also a one-to-one correspondence identifier, and it is marked as “trusted.” When the user disconnects, they are immediately re-marked as “untrusted.” In this way, a higher security is provided for the traditional single MAC binding authentication method.

The model generally consists of the following sections:

Authentication function section. To authenticate the terminal device, this document uses the RADIUS authentication server. The authentication server has large-scale authentication capabilities and has certain scalability. These features and technologies increase efficiency and streamline management processes.

The implementation flow chart of the certification part is shown in Figure 1:

When a user needs to connect to the network, it connects to the AP first to authenticate its identity. When authenticating the identity, the required key will be distributed by the authentication server to the user. Of course, any user will be assigned a different key when connecting to the network to determine the uniqueness of the user, thus also protecting the security of the user’s data transmission. The keys here are redistributed and used each time the user reconnects to the network, which greatly increases security and reduces the likelihood of being attacked. All user-connected data are encrypted and stored in the corresponding device, and the authentication server retrieves and updates the data when it is authenticated.

Encryption function section. This article borrows the powerful data encapsulation and anti-attack capability of VPN and applies it to the wireless network, which greatly improves its security.

Security status management section. The security status is a security identifier unique to each device that is assigned by the authentication server when the user connects to the network. When a user is authenticated legally, the authentication server marks it as a trusted device. When the device is disconnected, the identity is re-updated to be untrustworthy until it is successfully re-authenticated.

The workflow of the dynamic model in this article: If users want to access the Internet, they need to submit an application, and these data will be encrypted by the VPN. If the device is accessing the network for the first time, the AP records its MAC address and sends the request to RADIUS. RADIUS will query the database. If it passes the authentication, it will notify the AP to assign IP and record the MAC and IP address. At the same time, it is assigned a trusted identifier. When a user disconnects from the network, the identifier is immediately updated to be untrustworthy. If the user reconnects, the authentication needs to be restarted. The biggest feature of the improved model in this article is the ability to combine the authentication process and VPN encryption technology to improve the security of wireless network connections.

Experiments

Dynamic security models can improve the security of connections. In order to verify the validity of the model, the following experiment will conduct a series of simulated attack tests and also a simple test of the performance loss caused by VPN encryption.

Experimental purpose

The first is to test the validity and reliability of the model. Since the development model of this article is for enterprise users, the effectiveness and reliability are the indicators that this article focuses on. This article uses a man-in-the-middle attack method and a session interception attack method to perform a comparative test.

The second is to discover problems in the system. The development of science is tortuous and needs to move forward from the problem. Therefore, it is another purpose of this article to find problems and find ways to improve them.
The third is to test the impact of the model on network communication capabilities. Due to the use of VPN encryption technology, there will be some impact on performance. As for the degree of impact on network performance, a test is required, and the impact result should be as low as possible.

Experimental environment and conditions

The experiment was tested in the laboratory. The detailed steps are as follows: There are 2 days of user equipment, both as a normal networked user and also install Shentong test software for simulated attacking. The Windows Server 2003 operating system is installed on the authentication server, and the Internet Authentication Server service is added. Then, the open source FreeRadius software is installed on it to be used as a RADIUS authentication server. Install a VPN client on the computer to implement VPN encrypted transmission. Sniffer is installed on the authentication server to implement dynamic monitoring of network data.

In the test, the two computers were attacked by means of intermediaries and session interception. During the attack, Sniffer is used to analyze the bandwidth data to calculate the impact of the model on the performance of the network bandwidth.

Experimental steps

The purpose of the system test was analyzed above. The following will test and analyze the middleman and session interception attacks, and test the impact of the model on network performance. The specific system security test flow chart in this article is shown in Figure 2:

Man-in-the-middle attack test. Test method: The principle is that the attacker illegally obtains the transmission data packet between the AP and the user through the penetration test software, and analyzes it. Since much information can be obtained in reverse, this method can obtain a lot of sensitive information. After obtaining the information, the attacker impersonates the legitimate user and connects to the AP.

The process of this test is as follows:
First install the man-in-the-middle attack software CAIN in the attack terminal B, and then use the software to scan and detect the internal LAN, and then test the man-in-the-middle attack mode in two cases.

The first method, that is, the case where VPN encryption is not used. After starting the attack, you can get sensitive information, and the user cannot detect the abnormality. But many access to confidential information has been obtained by attackers.

The second method uses a VPN encrypted connection. At this time, CAIN can still scan all the hosts in the LAN, but when further infiltration is initiated, the hacker cannot obtain any valid information due to the strong encryption of the VPN.

Session interception attack test. Test method: The purpose of the attack is to extract information transmitted between the user equipment, the AP, and the authentication server. The specific steps are as follows: the attacker uses the penetration test software to capture the data between the normal user and the AP and the authentication server, and extracts the key, and then finds a way to forcibly disconnect the normal user and replace it with a legitimate terminal user, to get greater operational privileges between LANs.

With the first method, the convolutional neural network (CNN) has been able to obtain the correspondence between the MAC address and the IP address, that is, the address resolution protocol (ARP) routing table. When the model of this article is enabled, because the
model has improved the authentication method of device connection, even if the attacker wants to disconnect the normal user, there is no way to deceive RADIUS.

**Network performance test**. Testing for network performance involves two aspects. The first is to test the device connection authentication speed and network access speed after the VPN is turned on. The second is to test the bandwidth transmission of network traffic after the model is turned on, and compare it with the unopened.

**Discussion**

**Experimental results and analysis**

**Man-in-the-middle attack test**. According to the above detection method, 32 computers were tested in this article. This article uses the CAIN penetration test software to make a statistics on the attack success rate in both the state of opening and closing the VPN. The result is shown in Figure 3:

Analysis of test results: This attack method works only when the 802.1x protocol is transmitted in plain text or when the key is deciphered. Of course, cracking the key requires a lot of computing power. Since the system uses VPN encryption and the key is constantly updated, this method does not work for this system. The results of the above experiments are a good illustration of this.
Session interception attack test. According to the experimental method described above, this article simulates attacking 32 computers. The resulting comparison table is shown in Figure 4:

Analysis of test results: As the attack method works, the premise is that only the MAC address is used for network authentication. Since the system not only uses MAC address authentication, but also adds two bases of IP address and security identifier to jointly determine the legitimacy of the connection, the traditional session interception attack cannot be effective. The results of the above experiments are also a good illustration of this.

Network performance test. During the test, there are many parameters that can indicate the speed of the network. This article selects several representative parameters, which are

- Number of successful responses per unit time: Times;
- Number of clients accessing the gateway at the same time: Number;
- Total test usage time: SumTime;
- Response time of the VPN authentication server: ResTime;
- Processing rate of the VPN authentication server: Rate;

Table 1. Experimental results under a single VPN.

| Times | Number | SumTime | ResTime | Rate  | HNum  | LongTime | ShortTime |
|-------|--------|---------|---------|-------|-------|----------|-----------|
| 300   | 170    | 64.13   | 27.49   | 4.14  | 131.88| 63.67    | 0.3       |
| 400   | 210    | 79.18   | 28.98   | 4.93  | 177.66| 68.88    | 0.42      |
| 500   | 260    | 104.9   | 38.54   | 4.26  | 234.42| 95.79    | 0.61      |

VPN: virtual private network.

Maximum number of concurrent connections during the test: HNum;
The maximum time for a single response during the test: LongTime;
The shortest time for a single response during the test: ShortTime.

The results of the test are shown in Table 1 and Figure 5:

After the improved model of this article, the results of the processing are shown in Table 2 and Figure 6:

Analysis of test results: From the above experimental results, it can be found that in the case of using a single VPN, because the resources of a single machine are limited, when a high concurrent connection is made, it is prone to insufficient memory. After the improvement of this article, the load balancing technology is used, and the processing tasks are evenly distributed to each machine, which can effectively improve the processing speed. It can be seen that the improved method of this article is effective.

The statistics of the network traffic load under the system are turned on and off. The statistics obtained are shown in Figure 7:

Analysis of test results: As can be seen from Figure 8, when the security system is turned on, the
The proportion of valid data in the system is 79.49%; when the security system is turned off, the effective data ratio is only 56.84%. Therefore, although the system enhances the security, it still imposes a certain load on the traffic, which is also a place where the system needs further improvement.

**Conclusion**

Since the wireless network has obvious portability with respect to the wired network, the network access method is widely used, and at the same time, it is more vulnerable to attack by criminals. In order to solve the security problem, the security solutions proposed in the early years (such as WEP) have been unable to adapt to the growing network security needs. Therefore, it is necessary to build a more secure dynamic model.

This article studies the operation process of RC4 algorithm and AES algorithm, and proposes an improved scheme. In this article, based on the inherent MAC address filtering technology of wireless network card, a dynamic security model of wireless network is proposed and constructed. Devices accessing the network use the 802.1x authentication method and assign and set security state values for each device. The authentication server uses RADIUS. This article uses the VPN encryption network method to provide an encryption layer for communication between the device and the wireless network, so as to be able to encrypt and protect the data in the network transmission. This article changes the structure and policy of RADIUS to ensure the high security of wireless network devices in the connection process. In the testing phase of this article, we conducted several detailed tests on the model. The test is divided into a middleman and a session interception test. A large number of test results show that the model in this article can improve the security of wireless networks and have good performance.

Although this article solves a lot of security issues, there are still many areas that need improvement. (1) Although the VPN encryption technology used has improved security, it also brings about an increase in...
cost. (2) Considering the technical complexity and cost, there is no improvement in the data backup of the authentication server. So this part is the direction that needs to continue to work hard. (3) The model proposed in this article focuses on the security hardening of the server side, and does not make better suggestions for the security of the client. So how to improve the security performance on the client is the further research direction of this article.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD
Yuanming Li https://orcid.org/0000-0002-5210-8705

References
1. Wei Z, Wu H, Xin Y, et al. Achievable capacity scaling laws of three-dimensional wireless social networks. *IEEE T Veh Technol* 2018; 11(9): 2671–2685.
2. Hlavacek D and Chang JM. A layered approach to cognitive radio network security: a survey. *Comput Netw* 2014; 75(1): 414–436.
3. Min X, Tao X, Fan Y, et al. Enhancing secured coverage with CoMP transmission in heterogeneous cellular networks. *IEEE Commun Lett* 2016; 20(11): 2272–2275.
4. Na L, Tao X, Wu H, et al. Large-system analysis of artificial-noise-assisted communication in the multiuser downlink: ergodic secrecy sum rate and optimal power allocation. *IEEE T Veh Technol* 2016; 65(9): 7036–7050.
5. Wang C, Zhao Z, Gong L, et al. A distributed anomaly detection system for in-vehicle network using HTM. *IEEE Access* 2018; 6: 9091–9098.
6. Agrawal N and Tapaswi S. Wireless rogue access point detection using shadow Honeynet. *Wirel Personal Commun* 2015; 83(1): 551–570.
7. Hu B and Gharavi H. Smart grid mesh network security using dynamic key distribution with Merkle tree 4-way handshaking. *IEEE T Smart Grid* 2014; 5(2): 550–558.
8. Dong J and Kim WJ. Experimental analysis and implementation of a multiscale wireless/wired networked control system. *Int J Control Autom Syst* 2014; 12(1): 102–110.
9. Misra S. The future of wireless networks: architectures, protocols and services (Guizani, M., et al.; 2015)[book review]. *IEEE Wirel Commun* 2016; 23(1): 8–9.
10. Fragouli C, Prabhakaran VM, Czap L, et al. Wireless network security: building on erasures. *Proc IEEE* 2015; 103(10): 1826–1840.
11. Reza AW, Dimyati K, Noordin KA, et al. A comprehensive study of optimization algorithm for wireless coverage in indoor area. *Optim Lett* 2014; 8(1): 145–157.
12. Kwon DS, Yeo TD, Oh KS, et al. Dual resonance frequency selective loop of near-field wireless charging and communications systems for portable device. *IEEE Micro Wirel Co* 2015; 25(9): 624–626.
13. Pedersen J, Amat AGI, Andriyanova I, et al. Distributed storage in mobile wireless networks with device-to-device communication. *IEEE T Commun* 2016; 64(11): 4862–4878.
14. Omala AA, Kibiwott KP and Li F. An efficient remote authentication scheme for wireless body area network. *J Med Syst* *Wirel Commun* 2017; 41(2): 25.
15. Xiong N, Yang F, Li HY, et al. Security analysis and improvements of IEEE Standard 802.16 in next generation wireless metropolitan access network. *Wirel Commun Mob Comput* 2016; 11(2): 163–175.
16. Blumenthal U, Marcovici M, Mizikovsky S, et al. Wireless network security architecture. *Bell Labs Tech J* 2014; 7(2): 19–36.
17. Izhar M, Shahid M and Singh V. Network security issues in context of RSNA and firewall. *Int J Comput Appl* 2014; 82(16): 33–38.
18. Ito R and Miyagi A. Refined Rc4 Key Correlations of Internal States in WPA. *IEICE T Fund Electr* 2015; 21(6): 1132–1144.
19. Xia WY, Wu KJ and Zhou L. The security analysis of WLAN protocol based on 802.11i. *Appl Mech Mater* 2014; 32(7): 513–517.
20. Robyns P, Bonne B, Quax P, et al. Short paper: exploiting WPA2-enterprise vendor implementation weaknesses through challenge response oracles. *Proc ASME* 2014; 13(5): 189–194.