2018 15th International Symposium on Pervasive Systems, Algorithms and Networks

The Wi-Fi Device Authentication Method based on Information Hiding

Wei Liu
School of Computer Science
BUPT
Beijing, China
wliu@bupt.edu.cn

Zhehao Yan
School of computer Science
BUPT
Beijing, China
yanzhehao454@bupt.edu.cn

Yunhua He
School of Computer Science
NCUT
Beijing, China
heyunhua@ncut.edu.cn

***Abstract*—For smart home scenarios with using of Wi-Fi communication, users may want to access or control smart terminals by connecting gateway with user devices such as mobile phones. However, such the connection lacks the authentication step of user device, so this communication is likely to be eavesdropped by attackers. This paper proposes a device authentication method to access to the gateway based on information hiding channel. The device performs identity identification and permission control to achieve secure and efficient data transmission between user device (mobile phone) and gateway. The method uses elliptic curve encryption algorithm to encrypt communication data, and put key negotiation process into the frame bodies of several randomly specified MAC layer data frames. Under the condition of ensuring security, the efficiency of hidden communication is improved. The result of security analysis proves that this method has scalability and can resist physical capture attacks and Sybil attacks to a certain extent.**

Keywords—Wi-Fi, devices authentication, information hiding, communication security

I. Introduction

With the advancement of technology, Wi-Fi technology has been popularized in many areas, and many applications derived from this technology have become more mature, especially in smart home field. Wi-Fi-based IoT home applications takes a mainstream part of market. Shows in Fig. 1, the common Wi-Fi smart home system consists of a remote server, a gateway and many smart terminals [1]-[2] such as a smart thermostat, light bulbs and so on. Users can access and control the smart terminals using user devices such as mobile phones by access to gateway.

As the medium for user to access to smart terminals, gateway is responsible for authenticating user device and monitoring the communication between user device and smart terminals. One way to identify user device is authenticating it before connecting to gateway. Only the device which have passed the identification check can access to and control smart terminals. Plus, since the openness of Wi-Fi communication channel, for the sake of security, the communication data between user device and gateway needs to be encrypted. According to different encryption systems, commonly used session key negotiation and management methods can be divided into symmetric key management and asymmetric key management [3]. The use of these key negotiation methods effectively increases the difficulty to analyze eavesdropped data for attackers.

But there are still privacy issues. Because the quantity of key negotiation methods is limited, attackers can use traffic analysis attack methods [4] to statistically analyze eavesdropped data, compare to the steps in data negotiation and guess which data negotiation method is used. So that they can know the exact data negotiation method and transmission mode. In this way, even if attackers don't know the key for encrypting data, they could know which data transaction may represent which step in the key negotiation method and thus they can inject destructive data into the network targetedly [5] in order to make the key negotiation process unable to proceed normally.

For consideration of above issues, we combine hidden communication with device authentication and propose a Wi-Fi device authentication method based on information hiding. Specifically, our method adopts an anonymous key negotiation method based on bilinear elliptic curve encryption algorithm, and hides the identity check process with information hiding technology. Based on normal data exchange process, 4 frame packets are picked randomly from the original data frame stream as the carrier of information hiding, so that identity authentication process is perfectly hidden and a secure identity authentication and key agreement method is realized.

The main contributions of this paper are:

1. We analyze the Wi-Fi transmission procedures and frame format in Media Access Control (MAC) Layer, and build a device authentication system based on hidden communication;

2. We combining hidden communication with key negotiation, proposes a Wi-Fi device authentication method based on information hiding. We find the balance point between security and efficiency, and reduces the data leakage possibility while keeps relatively high efficiency;

3. We analyze and compare our method against main exist schemes, with respect to different criteria: information hiding way, calculation overhead and communication overhead. And security analysis and performance evaluation proves that our method can resist physical capture attack and Sybil attack to some extent.

The structure of this paper is as follows: Section □ summarizes and analyzes existing identity authentication and key agreement protocols in related fields; Section □ gives a brief introduction to basic knowledge required for our method; Section □ describes in detail the specific design of Wi-Fi device authentication method based on information hiding; Section □ carries out the security analysis and performance evaluation of this method; Section □ summarizes the full text content.

II. Related work

As shown in Fig. 1, in smart home area, common IoT solutions include remote server, gateway and many smart terminals. When users want to control smart terminals, they can use device such as mobile phone to connect with the gateway. The commonly used security strategy in this process is encryption and authentication mechanisms [6]. At present, the research on WSN key agreement protocols at home and abroad is mainly divided into identity-based key system and certificate-based key system [7].

2375-527X/18/$31.00 ©2018 IEEE
DOI 10.1109/I-SPAN.2018.00022

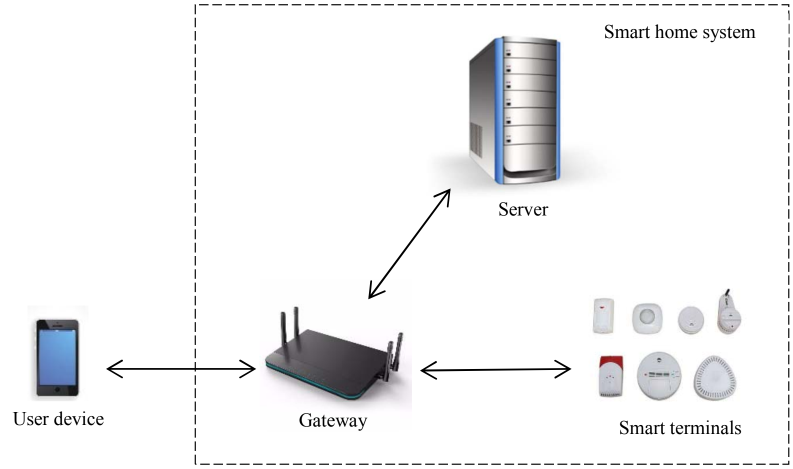

Fig. 1 Smart home system

2B	2B	6B	6B	6B	2B	6B	0-2312B	4B
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Seq-ctl	Address 4	Frame body	FCS

Fig. 2 Frame structure

Since the certificate guarantees the correspondence between holder and public key, it's relatively complicated when involves the management, issuance and revocation of certificates. In the identity-based key system, WANG et al.[8] made use of Gentry's identity-based encryption scheme and proposed the first key model protocol for certificate-based security. LAW et al. [9] proposed the ECDH-based encryption. The key exchange protocol, using implicit authentication, implements identity authentication and key negotiation for both parties of the communication. The improved protocol proposed by [10] has higher security and it can effectively resist man-in-the-middle (MITM) attacks. Reference [9-11] proposed an ECC-based key agreement protocol for WSN. Compared with the DH algorithm, under the same security strength, the key length required by the ECDH protocol is shorter. And the requirements for computing power and storage are smaller. So it is more suitable for wireless sensor network environments with limited resources in all aspects.

The above authentication key agreement protocol does not fully consider the problem of privacy leakage during communication. As mentioned in [1], for small-scale smart home system, attackers are more likely to perform side channel attacks on sensors and other devices [12-13], and it is easier to collect more sensitive information than traditional personal computers. How to ensure the safe transmission without revealing user privacy is a problem which needs to be fully considered.

For the privacy issue in the communication process, Szczypiorski [14] proposed a data steganography system at the data link layer; Xiao X et al. [15] proposed a novel secure transmission strategy based on information hiding, using data pairs. This mapping method replaces the traditional encryption method for secure transmission. On the basis of [15], Wang B et al. [16] added the unique feature information that identifies the sensor in the information, so that the malicious node can be detected.

The method proposed in this paper integrates many classic ideas for solving problems, combining identity authentication, key agreement and hidden communication within smart home scenarios, and the proposed Wi-Fi device authentication method based on information hiding has both relatively high security and efficiency.

III. BACKGROUND

This section briefly introduces the basic knowledge involved in this paper.

A. Wi-Fi protocol frame structure

Wi-Fi is a subset of the 802.11 standard and is managed by the Wi-Fi Alliance. The 802.11 standard divides all data packets in Medium Access Control (MAC) layer into three types: data frames, management frames, and control frames. The management frames are responsible for controlling network management functions, including network operations such as devices joining or exiting in wireless networks.

The frame structure of management frame is shown in Fig. 2, and there are 14 reserved bits in Duration/ID field.

In our method, two devices (mobile phone and gateway) generate two 6 bits random numbers respectively and put them on 12 of the 14 reserved bits. The random numbers represent corresponding ordinal data frames. These selected data frames serve as a carrier for authentication information. That means real data is stored in the frame body of these data frames so as to fully conceal the authentication process.

B. Process of Wi-Fi connection

The two-device connection process in Wi-Fi is divided into three steps: scan, authentication, and connection.

- Scan: Access Point (AP) broadcast a beacon frame to all the stations (STA). There are network necessary information such as BSSID and SSID of the AP included in beacon frames. STA can detect the network by periodically listening to the Beacon frame.

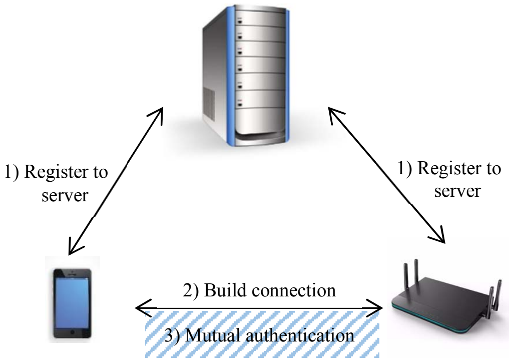

Fig. 3 Device authentication method

- Authentication: There are two modes for authentication -- open-system authentication and shared-key authentication. The former is equivalent to no authentication, thus there is no security protection at this step; the latter one uses certain encryption algorithms (such as WEP, WPA2, etc.) to encrypt data. In this step, the communication between both parties uses specific management frame type-- authentication request and authentication response.
- Association: The main operations in this phase is negotiation of communication parameters and establishment of channels between two parties. Once the connection is built, both parties can communicate by data frames.

C. Elliptic curve discrete logarithm problem

Given the elliptic curve $E(Fq)$ and the base point G on the finite field Fq, the order of G is k and k is a large prime number.

- Given an integer x, it is easy to calculate the point Q to make $Q = xP$;
- Given a point Q, it's very difficult to calculate an integer x to make $Q = xP$.

D. Bilinear mapping

Given G_1 and G_2 are cyclic groups with two large prime orders q. If $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear map, then for $a, b \in Z_q, P, Q \in G_1$, there are $e(aP,bQ)=e(P,Q)^{ab}$.

Specifically, in this paper, N_D and N_G are the name of the user device (mobile phone) and the gateway respectively, t is the master key corresponding to user identity group which the user device belongs to. User device keeps (N_D, tN_D), and the gateway keeps (N_G, tN_G). User device calculate key = $e(tN_D,N_G) = e(N_D,N_G)^t = e(N_D,tN_G)$ = the key calculated by the gateway, so both parties could get the same session key.

The key agreement protocol adopted in this paper is based on bilinear pairing on elliptic curve. The security of this key agreement protocol rests on the bilinear Diffie-Hellman assumption.

E. Security model

Based on a well-known security model for key exchange schemes [17], we define the security model for our methods as follows. In the hidden secondary authentication phase, every participant is either a client $C \in Client$ or an application provider $AP \in ApplicationProvider$ and C gets a secret key from server. Let A and Γ^idenote a probabilistic polynomial-time adversary and the i^{th} instance of a participant Γ, respectively, where Γ is a client or an application provider. The security of the authentication scheme is defined according to a game between a challenger A and a simulator S. A could make the following queries.

1) $h(m)$: Upon receiving a query, S first checks whether a tuple (m, r) is in L_h. If so, S returns r to A; otherwise, S generates a number $r \in Z_q^*$randomly, inserts the tuple (m, r) into L_h and returns r to A.

2) $H(m)$: Upon receiving the query, S first checks whether a tuple (m, R) in L_h. If so, S returns R to A; otherwise, S generates an element $R \in G_1$ randomly, inserts (m, R) into L_h and returns R to A.

3) SymEnc([e, d], k, [m, c]): Upon receiving an encryption query SymEnc(e, k, m), S first checks if there is a tuple (k, m, c) in the list L_{sym}; If so, S returns c to A; otherwise, S generates a random number c, records (k, m, c) into L_{sym}, and returns c to A. Similarly, upon receiving a decryption query SymEnc(d, k, c), S first checks if there is a tuple (k, m, c) in the list L_{sym}; If so, S returns m to A; otherwise, S generates a random number m, records (k, m, c) into L_{sym}, and returns m to A.

4) Create(C, $right$): Upon receiving the query, S generates the secret key of C with the right parameter. 5) Create(AP): Upon receiving the query, S generates the private/public key pair of AP and returns the generated public key to

6) Send(Γ^i , m): Upon receiving the query, S executes steps in our method and outputs corresponding message.

7) Reveal(Γ^i): Upon receiving the query, S returns the session key of the participant instance Γ^i to A.

8) Corrupt(Γ): Upon receiving the query, S outputs the secret key of Γ to A.

9) Test(Γ^i): Upon receiving the query, S chooses a random bit $b \in \{0, 1\}$. If b = 1, S returns the session key of Γ^i to A; otherwise (b = 0), S generates a random number and returns it to A.

An instance Γ^i is accepted when it receives the final message and turns into some intended mode. The session identification (sid) of the instance Γ^i is defined as the concatenation of all messages sent and received by Γ^i.

Two instances $C^i$and AP^j are partnered if none of the following conditions does not hold: 1) both of $C^i$and AP^j are accepted; 2) both $C^i$and AP^j have the same sid; and 3) $C^i$and AP^j are partner of AP^j and C^i separately.

An instance Γ^i is fresh if none of the following conditions does not hold: 1) $\Gamma^i$is accepted; 2) there is no Reveal that has been made to Γ^i or its partner; and 3) there is no Corrupt that has been made to Γ^i or its partner.

Let Succ(A) denote the event that A could guess the correct bit b ∈ {0, 1} involved in Test query. The advantage of A violates the indistinguishability of the scheme Ψ which is defined as $Adv_{\Psi}^{AKE}(A) = |2\Pr[Succ(A)] - 1|$.

Definition 1: We say that an authentication scheme Ψ is authenticated key agreement (AKA)-secure if $Adv_{\Psi}^{AKE}(A)$ is negligible.

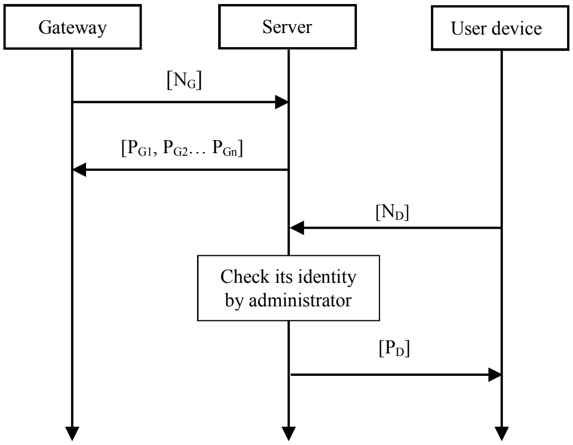

Fig. 4 Initialization step

We say that A could violate C − to − AP authentication of an authentication scheme Ψ if A could generate a login message. We say that A could violate the AP − to − C authentication of an authentication scheme Ψ if A could generate a response message. Let $Adv_{\Psi}^{AKE}(A)$ denote the probability that A could violate C − to − AP authentication and AP − to − C authentication of an authentication scheme Ψ.

Definition 2: We say that an authentication scheme Ψ is mutual authentication (MA)-secure if the probability $Adv_{\Psi}^{AKE}(A)$ is negligible.

IV. Wi-Fi Device hidden Authentication Method

This section mainly introduces the design ideas of Wi-Fi Device Authentication Method Based on Information Hiding.

This method decides whether the identities of user device and gateway are certified by verifying if these two parties have same group master key or not. Specifically, as shown in Fig.3, this method mainly includes three steps: system initialization, normal connection, and secondary authentication.

Gateway and user device needs to be registered on server first. Then administrator (owner of the smart home system) classifies the user device into one of groups, and server sends corresponding group master key to user device. When user device wants to get access to smart terminals, it needs to make normal connection with gateway through Wi-Fi first, then secret secondary authentication is performed. In secret secondary authentication step, if two parties have the same group master key, they can get the same session key. Only in this way, gateway would allow the user device to access and control smart terminal.

A. System establishment

This section is used to select several parameters required by system and complete the system initialization steps. The elliptic group *G* is a cyclic group with a large prime number *q* ($q>2^k$, *k* is a safety parameter); $H_1(a)$ is a hash function which can map any string *a* to an elliptic curve.

Since administrator have different relationship with different people (such as families, close friends, co-workers, etc.), it is expected that they have different authorities, such as reading and setting authority of all smart terminals, reading and setting authority of part of smart terminals, or just reading authority of some smart terminals. So the user devices can be divided into different groups according to different authorities, and members in the same group share a group master key. It needs to be pointed out that this method does not specify the quantity of divided groups, administrator could set the number of group and corresponding authority freely.

So according to the relationship between the user and the owner is close or not, the user device would be divided into a group with certain authority. Each group has different group master key: $k_1, k_2,..., k_n \in Z_q$. Members within the same group have same master key.

B. Secret Authentication Protocol

The Wi-Fi Device Authentication Method proposed in this paper mainly includes three steps: initialization, Wi-Fi connection, and secret secondary authentication.

a) *Initialization:* The main work of this phase is server registration process of gateway and user device. Gateway and user device register to server first, then server check their identity and if they are legal, server distributes master key to two parties.

As shown in Fig. 4, for gateway, the process of registering to server mainly includes the following steps:

1) Gateway randomly generates a 20B-length string, stores it as its name N_G, and sends N_G to server for registration request;

2) Server receives the gateway name and stores it. Then according to the formula $P_{Gi}=H_1(N_G)$ • t_i, server maps gateway name N_G to a point in elliptic curve through the hash function H_1（A）, multiplied the point with every master key $[k_1, k_2, ..., k_n]$ and then get $[P_{G1}, P_{G2}, ..., P_{Gn}]$. After that server stores these products and return them to gateway, and accomplish the registration process of gateway.

For user device, the process of registering to server mainly includes the following steps:

1) User device sends its 20B-length name N_D to server for registration request;

2) Server receives the data sent by user device, stores them as N_D, and sends it to administrator device. Then administrator checks the identity of this device, divides it into one of groups and returns the result to server;

3) After receiving identity group the user device belongs to, server maps N_D to a point in elliptic curve through hash function $H_1()$, and multiplies the point with corresponding group master key, then returns the product P_D to user device and accomplish the registration of user device.

b) *Wi-Fi connection:* What is completed in this stage is normal Wi-Fi connection process between user device and gateway with a little bit change. Section 3.2 shows the details of normal connection. Different from the normal Wi-Fi connection process, user device and gateway both generate two 6bit-length random numbers during the Authentication phase, and these numbers are put in 12-bit reserved bits in Duration/ID field of the

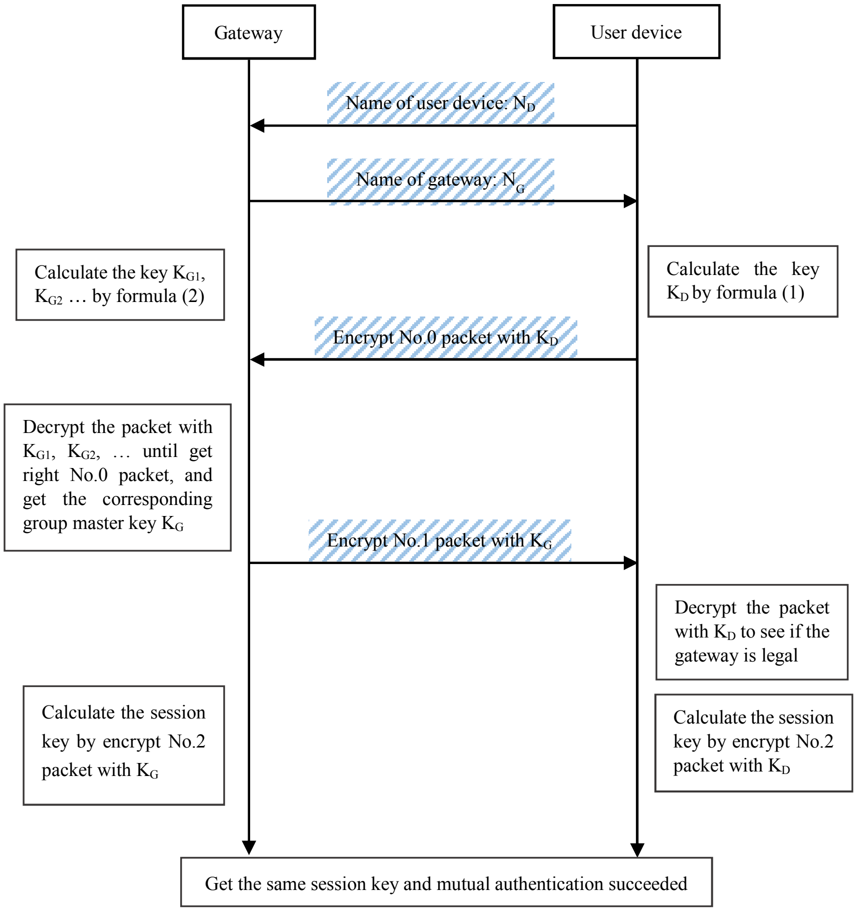
Gateway
User device
Name of user device: N_D
Name of gateway: N_G
Calculate the key K_{G1}, K_{G2} … by formula (2)
Calculate the key K_D by formula (1)
Encrypt No.0 packet with K_D
Decrypt the packet with K_{G1}, K_{G2}, … until get right No.0 packet, and get the corresponding group master key K_G
Encrypt No.1 packet with K_G
Decrypt the packet with K_D to see if the gateway is legal
Calculate the session key by encrypt No.2 packet with K_G
Calculate the session key by encrypt No.2 packet with K_D
Get the same session key and mutual authentication succeeded

Fig. 5 Hidden secondary authentication

MAC layer management frame. As management frames are transmitted to and from the other device, two parties negotiate four random numbers. The value of these random numbers represents some serial number of data frames. These selected data frames serve as the carrier for the hidden identity authentication process. The real data is put in frame body area of these data frames to fully conceal the key negotiation process.

By the way, because different systems have different security requirements, the number of random numbers can be reduced in situations where the efficiency requirements are high and the security requirements are general. If the length of random digits is n, the efficiency of this method is $4/2^n$;

c) *Hidden secondary authentication:* After user device and gateway completing the normal Wi-Fi connection and negotiating 4 random numbers, the secondary authentication phase is performed. The data transfer in this stage is based on hiding information. The carrier of hiding information is the frame body area of certain data frames specified by the 4 negotiated numbers.

As shown in Fig. 5, using the hiding information method described above, the secondary authentication process is as follows:

1) User device and gateway exchange their names respectively. User device calculates a key K_D according to the formula $K = e(P_D, H_1(N_G))$;

2) User device encrypts the Number 0 packet with K_D and sends it to gateway;

3) Because gateway keeps all the master keys of user device groups, the gateway uses the formula $K_{Gi} = e(H_1(N_D), P_{Gi})$ to calculate several keys $K_{G1}, K_{G2},..., K_{Gn}$. Gateway receives the data packet and uses $K_{G1}, K_{G2},..., K_{Gn}$ to decrypt the data one by one. When the decrypted packet equals to Number 0 packet, the user device is determined to be a legal device, and gateway could confirm which group the device belongs to according to this right key. Then gateway encrypts Number 1 packet with the right key and sends it to user device;

4) After user device receives the data sent by gateway, it decrypts the packet by the key K. If the decrypted result equals to Number 1 packet, it is considered that the gateway already knows its class, and at the same time, the conclusion that the gateway is credible is obtained;

5) After both parties confirm that the other party's identity is trusted, they encrypt the Number 2 packet with their own key as the subsequent session key. It is worth mentioning that if there is a higher security requirement, both parties can also change the session key uniformly

by encrypting data packets Numbers 3, 4, 5⋯ to enhance the security of communication;

6) In the process of negotiation, if any step of verification/decryption fails, it is necessary to return a data packet whose frame body is all 0 to the other party to notify it that the negotiation has failed. At this point, the secondary certification process is over.

C. *Correctness analysis*

This section describes the correctness of our device authentication method.

(1) Verification of the validity of key holder

The legality of the key is guaranteed when user device and gateway register to server. Only the server authenticates them as legal devices, the group master key will be distributed.

(2) Negotiation key consistency

User device key calculation is

$$
\begin{aligned}
K_{Gi} &= e\,(P_D，N_G) \\
&= e\,(tH_1(N_D),H_1(N_{Gi})) \\
&= e\,(H_1(N_D),H_1(D_{Gi}))^t \\
&= e\,(H_1(N_D),tH_1(D_{Gi})) \\
&= e(H_1(ND)，P_G) \\
&= K_G
\end{aligned}
$$

That is exact gateway key, so it can be considered that two devices having the same group master key *t* have the same key, thereby proving that both devices are legal.

D. *Management of key and responsibility*

User device master key is only explicitly stored by the server. On the gateway and user device, master key is kept in the form of $P = H_1(Name)t$ (product of master key and the hashed point of its name). That is, neither the user device nor the gateway knows the specific value of master key. This greatly reduces the probability that attackers obtain the master key through reverse parsing after the device is stolen, and effectively ensure the security of the master key.

When gateway discovers that user device has requested non-privilege operations for several times, it judges the situation as abnormal and reports the device name and the requested permission to server. After receiving the gateway's warning message, the server sends a message to administrator (the owner of the smart home system) to get confirmation of the group which the warning user device belongs to. If it is determined that this user device indeed exceeds the scope of its authority, the user device will be added to the blacklist. After blacklist is sent to gateway, the gateway could prohibit the access from this user device.

V. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

This section gives security analysis and performance evaluation.

A. *Security Analysis*

Suppose the adversary is a privileged insider of AP or a powerful hacker. The adversary could impersonate *C* to AP by executing the following process.

1) The adversary chooses a number $\omega \in Z_q^*$ randomly and calculates $ind_{C_v} = e(P,P)^{\omega}$, $\mathrm{I} = ind_{C_v} \cdot P$. The adversary stores the tuple {I, ind_{C_v} , right} in AP's database or uses it to replace some such a tuple in AP's database.

2) The adversary generates three random numbers *k, t, ξ* $\in Z_q^*$ and calculates $\mathrm{T} = \mathrm{t} \cdot \mathrm{P}, \mathrm{T}' = \mathrm{t} \cdot Q_{AP}, I' = I + T, r = e(P,P)^{\xi}, v = h(t_c, r, T), U = \xi \cdot P - \omega \cdot v \cdot P$, where t_c denotes the current timestamp. Finally, the adversary sends the message $\{\mathrm{v}, \mathrm{U}, t_c, \mathrm{T}', \mathrm{I}'\}$.

Next, we demonstrate that the message $\{\mathrm{v}, \mathrm{U}, t_c, \mathrm{T}', \mathrm{I}'\}$ could pass AP's verification. Since $ind_{C_v} = e(P,P)^{\omega}$, $\mathrm{I} = ind_{C_v} \cdot P$ $r = e(P,P)^{\xi}, v = h(t_c, r, T), U = \xi \cdot P - \omega \cdot v \cdot P$, we could get

$$
\begin{aligned}
&\mathrm{e}(\mathrm{U},\mathrm{P}) \cdot ind_{C_v}^{v} \\
&= e(\xi \cdot P - \omega \cdot v \cdot P, P)(e(P,P)^{\omega})^{v} \\
&= e\big((\xi - \omega \cdot v) \cdot P, P\big)e(P,P)^{\omega \cdot v} \\
&= e(P,P)^{\xi - \omega \cdot v}e(P,P)^{\omega \cdot v} \\
&= e(P,P)^{\xi - \omega \cdot v + \omega \cdot v} \\
&= e(P,P)^{\xi} = r
\end{aligned}
$$

Then, AP will get the equation $\mathrm{v} = \mathrm{h}(t_c, \mathrm{r}, \mathrm{T})$ holds. Therefore, the message $\{ \mathrm{v}, \mathrm{U}, t_c, \mathrm{T}', \mathrm{I}' \}$ could pass AP's verification and the adversary could successfully impersonate the client to access services provided by AP.

According to our analysis above, a straightforward fix may be to ensure that all tuples {I, ind_{C_v}, right} stored in AP's database are legal, i.e., they are generated by server. To achieve this goal, we only need to require server to issue {I, ind_{C_v}, right, σ_v} instead of {I, ind_{C_v}, right, } to AP in the registration algorithm, where σ_v is a digital signature on the message { I, ind_{C_v}, right} and σ_v is generated by server using its secret key *s* and a secure signature scheme. Besides, we require that AP verifies the validity of { I, ind_{C_v} , right} before using it in the authentication algorithm, where AP uses server's public key Q_S and the signature scheme to verify the legitimacy of { I , ind_{C_v} ,, right}. With this simple modification, the adversary cannot generate a valid tuple { I, ind_{C_v} , right, σ_v }. As a result, the adversary cannot impersonate *C* to AP.

B. *Performance evaluation*

This section measures the performance of this method mainly from computational overhead aspect and communication overhead aspect.

On the computational cost, assuming that the computational computation of a multiplication (scalar) on the elliptic curve is e_1, the required computational overhead is $4e_1$ during an identity process.

In terms of communication overhead, the number of required data packets is mainly considered. Assuming that the communication overhead for sending and receiving a piece of data is e_2, e_3. In this method, the designation of the data frame serial number is randomly generated by the two devices, and is put into a reserved bit of the management frame after being generated, without bringing additional communication overhead. Both the gateway and the user terminal use a name length of 20B. The frame body of the data frame has enough space to accommodate the data. Therefore, according to the Fig. 5, the data exchange between the two parties includes the exchange of names, and the transmission of the encrypted data packets 0 and 1 is 4 in total. Thus the communication overhead of this method is $4(e_1+e_2)$. Since these 4 data frames are hidden in the normal data frame transmission, the effective efficiency of hidden communication is 12.5%. If the security requirements are high and the efficiency requirements are high, a random number with a small number of bits can be used to greatly improve the communication efficiency. In summary, the resources required to perform a key agreement are $4(e_1 + e_2 + e_3)$.

VI. Conclusion

Based on the problem of users want to access and control smart terminals through the gateway but lacks the effective authentication step in current smart home system. This paper proposes a Wi-Fi device identity authentication method based on hiding information. This method combine the hidden communication and authentication steps. When using Wi-Fi protocol to send and receive data, several random data frames are served as carriers for hidden communication process, so that both parties can complete mutual authentication and key agreement process more securely. At the same time, after security analysis and performance evaluation of our method, it proves that our method has scalability and can resist physical capture attack, complicity attack and Sybil attack to some extent. Compared with other protocols, this method requires equipment calculation and storage resources within a reasonable range. At the same time, it improves the efficiency of hidden communications without scarification of security, and is suitable for the authentication process in smart home which has pursuit of safety and efficiency.

Acknowledgment

The work was supported by National Natural Science Foundation of China under the grants of No.61602053, State Key Laboratory of Information Security(Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093)(2017-MS-14), and the Fundamental Research Funds for the Central Universities.

References

[1] Zhang Yuqing, Zhou Wei, Peng Anni. Survey of Internet of Things Security. Journal of Computer Research and Development, 2017, 54(10): 2130-2143

[2] Santoso, F. K., & Vun, N. C. (2015, June). Securing IoT for smart home system. In Consumer Electronics (ISCE), 2015 IEEE International Symposium on (pp. 1-2). IEEE.

[3] Michalevsky, Y., Nath, S., & Liu, J. (2016, October). MASHaBLE: mobile applications of secret handshakes over bluetooth LE. In Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking (pp. 387-400). ACM.

[4] Maple, C. (2017). Security and privacy in the internet of things. Journal of Cyber Policy, 2(2), 155-184.

[5] Balfanz, D., Durfee, G., Shankar, N., Smetters, D., Staddon, J., & Wong, H. C. (2003). Secret Handshakes from Pairing-Based Key Agreements. Security and Privacy, 2003. Proceedings. 2003 Symposium on (pp.180-196). IEEE.

[6] FANG Wei-dong, LI Feng-rong, SHAN Lian-hai,et al.Anonymous Communication Technology for Wireless Sensor Network: a Survey. Journal of Beijing University of Posts and Telecommunications, 2017,(1):1-17,27.

[7] Zeng, P., Zhang, L., Hu, R. L., Yang, Y., & Liu, P. (2014). Lightweight authenticated key agreement protocol based on ECC for wireless sensor networks. Comput. Eng. Applic, 50, 65-69.

[8] Wang, S., Cao, Z., & Dong, X. (2007). Provably secure identity-based authenticated key agreement protocols in the standard model. CHINESE JOURNAL OF COMPUTERS-CHINESE EDITION-, 30(10), 1842.

[9] Law, L., Menezes, A., Qu, M., Solinas, J., & Vanstone, S. (2003). An efficient protocol for authenticated key agreement. Designs, Codes and Cryptography, 28(2), 119-134.

[10] Shengjin, L., Changhong, Z., & Dawei, Z. (2011). An authenticated key agreement protocol based on ECDH. Information Security and Communications Privacy, 7, 70-72.

[11] McCann, D., Eder, K., & Oswald, E. (2015, September). Characterising and comparing the energy consumption of side channel attack countermeasures and lightweight cryptography on embedded devices. In Secure Internet of Things (SIoT), 2015 International Workshop on (pp. 65-71). IEEE.

[12] Conti, M., Nati, M., Rotundo, E., & Spolaor, R. (2016, May). Mind the plug! Laptop-user recognition through power consumption. In Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security (pp. 37-44). ACM.

[13] Costin, A., Zaddach, J., Francillon, A., Balzarotti, D., & Antipolis, S. (2014, August). A Large-Scale Analysis of the Security of Embedded Firmwares. In USENIX Security Symposium (pp. 95-110).

[14] Szczypiorski, K. (2003, October). HICCUPS: Hidden communication system for corrupted networks. In International Multi-Conference on Advanced Computer Systems (pp. 31-40).

[15] Xiao, X., Sun, X., Yang, L., & Chen, M. (2007, August). Secure data transmission of wireless sensor network based on information hiding. In Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on (pp. 1-6). IEEE.

[16] Wang, B., Qian, H., Sun, X., Shen, J., & Xie, X. (2015). A Secure Data Transmission Scheme Based on Information Hiding in Wireless Sensor Networks. International Journal of Security and Its Applications, 9(1), 125-138.

[17] Bellare, M., Pointcheval, D., & Rogaway, P. (2000, May). Authenticated key exchange secure against dictionary attacks. In International conference on the theory and applications of cryptographic techniques (pp. 139-155). Springer, Berlin, Heidelberg.