A SECURE FAST HANDOFF SCHEME WITH ATTRIBUTE-BASED ACCESS CONTROL FOR SECURE ENTERPRISE WLAN

Meng Lv[1], Zhe Liu[1], Jianwei Liu[1], Qianhong Wu[1], Chengxiang Gong[2]
[1]School of Electronics and Information Engineering, Beihang University, Beijing 100191, China
[2]Beijing Selection Center, Beijing 100061, China
lvmeng11@hotmail.com,lzfirm@163.com,liujianwei@buaa.edu.cn,qianhong.wu@buaa.edu.cn，gongliang1105@163.com

Key words: WLAN, Fast Handoff, CP-ABE, Fine-grained, Security-requirement-oriented

Abstract

Because of its flexibility and convenience, WLAN has been an essential technology for enterprise Network. It becomes a heated issue to improve the performance of handoff process in public communication, but few works aimed to secure access control when a handoff occurs, which is crucial to data privacy protection, especially in secure communication or Data distributed storage system. In this paper, we propose a novel handoff scheme which uses attribute-based encryption to realize security requirement oriented access control. Only the authorized mobile station which satisfies the access control policy made by the new domain can access into the new access point. With our scheme, each domain is able to make its own access control policy to avoid private data being illegally used by unauthorized users.

To the best of our knowledge, this is the first secure handoff scheme equipped with security requirement oriented access control in handoff scheme. Security analysis shows that our scheme can effectively provide enterprise-level security. The experiment analysis indicates that the handoff process can be completed within 30ms, which is fast enough to support real time communication such as VoIP.

1 Introduction

Enterprise network is an enterprise-wide network that integrates the communications, processing, data storage all of the other resources of the corporation, then make the resources available to the users all over the corporation. [1] Data privacy and convenience to use are widely concerned as two extremely important issues of enterprise network.

Because of its support to mobility and strong scalability, Wireless LAN has been an essential technology for enterprise Network. In order to provide high-quality seamless network services, for a long time, researchers are concerned about designing enterprise-level secure and low-latency handoff scheme.

1.1 Related work

The IEEE 802.11 standard, a milestone of internet technology, has changed the way mobile device access the network. IEEE 802.11i [2] produced by task group I is the first universally accepted specification which provides enterprise-level security. [3] It uses IEEE 802.1X protocol to implement authentication but has a drawback that the length of time it takes to authenticate as a mobile user roam into a new access point(AP) is too long to support latency sensitive service. As real time service has been enjoying a boom, the issue of latency involved in a handoff from one access point to another has been well studied.

IEEE 802.11r [4] is a revision of 802.11i proposed to directly support faster roaming in the MAC protocol. It uses keying hierarchy to derive encryption keys and optimize the authentication process to minimize the latency of a roaming process. [12] Although 802.11r can achieve the authentication within 20ms in best case, unwanted leakage is not only an issue of key compromise but also a heavy burden on authentication server.

The Control and Provisioning of Wireless Access Point (CAPWAP) [5] which is standardized by the IETF in the form of RFCs is to provide a protocol to support enterprise WLAN environments. It employs a central authority and divides the APs into two logical components, which implements the upper MAC functionality of traditional APs by a centralized access controller. When roaming occurs, the AC can directly execute a new 4-way handshake and simply derive a new key. The drawbacks are same to 802.11r since it still uses key hierarchy to derive new keys.

Reference [6] proposes a secure fast roaming scheme named as SFRIC. It simplifies the authentication process by using ID-based Cryptography to allow a mobile user and an AP to establish a PTK without a pre-distributed PMK. However, it has DoS vulnerability and can only perform coarse-grained access control.

Yueming Deng et al. propose a fast authentication scheme, called T-FISH, which presents the idea of authentication based on a trust-token encrypted by ABE. [7] It is the first handoff scheme that using ABE but only support one-way authentication and the handoff latency is 2.863sec, which is intolerable for real time service.

It must be pointed out that, although lots of work has been done to improve enterprise WLAN, very little of them focus on the issue of access control and data privacy protection when a handoff occurs.

1.2 Our work

In this paper, we introduce a novel handoff scheme, which allows seamless handoff without requiring keys

pre-distribution to neighbor APs. And we show that it is an efficient scheme to use CP-ABE to implement flexible and fine-grained access control during a handoff. In our scheme, each domain specifies an access structure for an authentication token which is referred to the access control policy. Only mobile users with decryption keys whose associated attributes satisfy the access structure can decrypt the authentication token and access the domain.

In our construction, the domains don't need to know the identities of the users and mobile users can realize mutual authentication with visiting AP just by decrypting and verifying the authentication token issued by the visiting domain instead of re-authentication or requiring communication with other AP to derive keys, which effectively reduces the latency and prevents key compromise.

The rest of the paper is organized as follows. Section II provides the design goals of our scheme, an overview on CP-ABE and the background on groups equipped with bilinear maps. In Section 3, we present our scheme in detail. Then, we give the security analysis of our scheme in Section 4 and evaluate its performance based on real implementation in Section 5. Finally, we draw a conclusion in Section 6.

2 Preliminaries

2.1 System Architecture and Design Goals

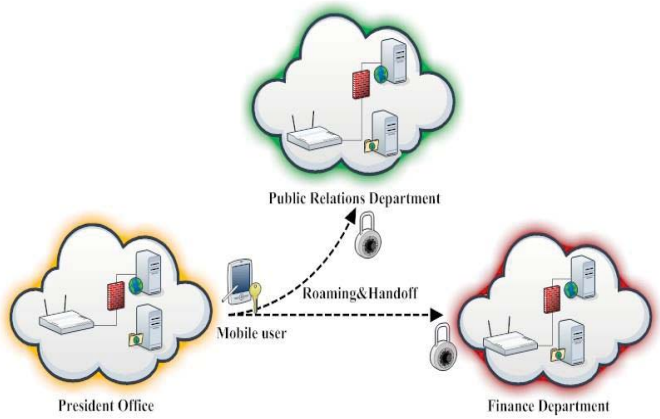

Figure 1. A scenario of enterprise WLAN

In enterprise network, sensitive data is generally stored in distributed servers of each relevant department and only the users who have the specific access priority can access the sensitive information. Figure 1 shows a typical scenario of enterprise wireless LAN. As the figure shows, each network domain is tagged with a security level according to the sensitivity of the information it stores (each security level is denoted with different color). In such a scenario, handoff scheme must satisfy the following requirements:

Autonomous policy creation. Make sure that each network domain is able to create access control policy autonomously according to the sensitivity of the information it stores.

Seamless handoff. Ensure the user who has the specific access priority can roam into new access point seamlessly without communication interruption.

Fine-grained access control. Refuse the access of users unable to satisfy the access control policy and protect the data privacy.

We define the handoff scheme which meets the above three conditions as security-requirement-oriented handoff scheme.

2.2 Ciphertext-Policy Attribute-Based Encryption

Bethencourt *et al.* proposed a new cryptosystem named as Ciphertext-Policy Attribute-based Encryption [9] which can be used to perform complex access control. In their CP-ABE scheme, attributes are used to describe the users, and the access structure is introduced to ensure that a user can access the message only if the user's private key which derived over its attributes satisfies the access structure implicitly contained in the ciphertext. A CP-ABE scheme consists of Setup, Encrypt, KeyGen and Decrypt as four basic algorithms which are briefly introduced as follows:

Setup (λ): The setup algorithm takes the security parameter λ as input, and outputs a master secret key MSK as well as a public key PK.

Encrypt (PK, M, 𝔸): It takes the public key PK, an access structure 𝔸 over the attributes universe, and a message M as inputs of the encryption algorithm. The function of encryption algorithm is to encrypt M then output the ciphertext CT. Only a party with a set of attributes which matches the access structure will be able to decrypt the ciphertext.

KeyGen (MSK, *S*): It takes MSK and a set of attributes *S* which describes the key as input. It outputs a private key SK for the set of attributes *S*.

Decrypt(PK, CT, SK): The public key PK, a private key SK for attributes set *S*, and ciphertext CT are taken as inputs of the decrypt algorithm. The algorithm will decrypt the ciphertext only if the set S matches the access structure 𝔸.

Access Structure: In our scheme, we use the same tree access as illustrated in reference [9]. In our tree access structure, we set that the non-leaf nodes represent threshold (denote threshold value as k_x, the number of children nodes as num_x , $0 < k_x \leq num_x$), while leaf nodes represent attributes. The threshold gate is an AND gate when $k_x = num_x$, while it is an OR gate when $k_x = 1$. Let $\mathcal{T}_x$ denote the tree of which root is node x. For a set of attributes S, we denote $\mathcal{T}_x(S) = 1$ only if S satisfies the access tree $\mathcal{T}_x$: if x is a non-leaf node, calculate $\mathcal{T}_{x'}(S)$ for all its children x′, $\mathcal{T}_x(S) = 1$ only if at least k_x children return 1.If x is a leaf node, then $\mathcal{T}_x(S) = 1$ if and only if att(x) ∈ S.

An example of the tree access structure is shown in Fig. 2, of which policy is defined as follow:

$$Policy\mathbb{A} = \big((STA\ level > 4)AND(Accounting)\big) \\ OR((President)AND(Beijing))$$

where the threshold values for 'OR' and 'AND' are 1 and$num_x = 2$, respectively. This access structure demands that only a staff in accounting department of level more than 4 or the president of Beijing branch can access the WLAN domain.

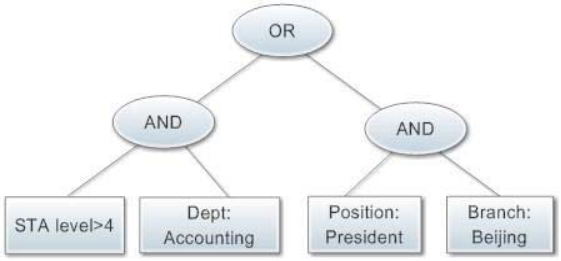

Figure 2. Example of access structure

2.3 Bilinear Maps

Bilinear groups are defined by a group generator g. Let $\mathbb{G}_0$ and $\mathbb{G}_1$ be two finite cyclic groups of prime order p, then the bilinear map e is defined as $e : \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$, which satisfying the properties as follows:

1. Bilinear: for all $g, h \in \mathbb{G}_0$ and $u, v \in \mathbb{Z}_p$, we have $e(g^u, h^v) = e(g, h)^{uv}$.
2. Non-degeneracy: $e(g, g) \neq 1$.
3. Computability: There exists an efficient algorithm to compute $e(g, h)$ for all $g, h \in \mathbb{G}_0$ in polynomial time.

2.4 PBC Library and CPABE Package

The PBC library is a free portable C library, built on top of the GMP library, allowing the rapid prototyping of pairing-based cryptosystems. It provides an abstract interface to a cyclic group with a bilinear pairing, insulating the programmer from mathematical details.

The cpabe toolkit [10], which has been made available on the web under the GPL, provides a set of programs implementing a Ciphertext-Policy Attribute-based Encryption scheme. The toolkit calls PBC library[11] for the algebraic operations and provides four command line tools: cpabe-setup, cpabe-keygen, cpabe-enc, cpabe-dec, which corresponding to the four fundamental algorithms used to perform the various operations of the scheme.

3 Our Construction

In our scheme, a domain authenticator specifies an access structure for a ciphertext which is referred to as the ciphertext policy. Only mobile stations with decryption keys whose associated attributes satisfy the access structure can decrypt the ciphertext.

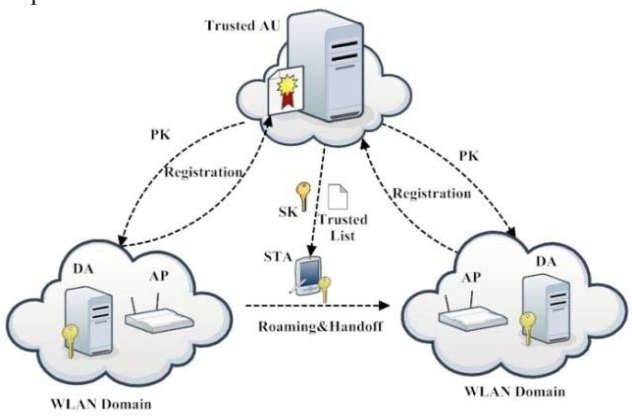

Figure 3. Our system model

3.1 System Model and Assumption

As depicted in Fig. 3, our system consists of 4 types of parties: trusted authority *AU,* a number of access points *AP*, domain authenticators *DA* and mobile stations *STA*.

We assume that STA in our construction has already implemented Initial Authentication in their home domain. Additionally, the *home access authenticator* will authorize a *priority-level* and sends a *home domain ID* to the STA in a secure channel if the initial authentication is successful.

The trusted authority, acting as the root of trust, is responsible for implementing Setup and KeyGen algorithm to generate and distribute public parameter, master key and a private key. Additionally, we set that each domain authenticator should be authenticated by the trusted authority

Each domain authenticator is associated a public key and a private key, with the former being made public and the latter being kept secretly by the party. A domain authenticator is responsible for implementing Encrypt algorithm and sending an *auth-token* massage to the mobile station which is willing to roam.

A mobile station which is willing to roam should get a private key assigned by the trusted authority. It is responsible for decrypting *CT* and verifying the identity of visiting DA.

3.2 Attributed-based Secure Fast Roaming Scheme

System Initialization

First, we suppose that every domain authenticator should be authenticated by the trusted authority in the stage of system initialization. If authenticated, each trusted domain authenticator will be assigned a public key pk_i, a private key $privk_i$ and a *domain priority-level,* here i represents the number of the domain. Then the trusted authority will create a Trusted-List which includes registration information of each trusted domain authenticators as

$$regis_i = \{ID || h_i = hash(pk_i)\}$$

Recall that we have mentioned four algorithms in above: Setup, KeyGen, Encrypt, Decrypt. Now we describe the main operations of our scheme in detail.

In our scheme, it consists of two phases for an STA intending to roam from its home domain to another visiting domain.

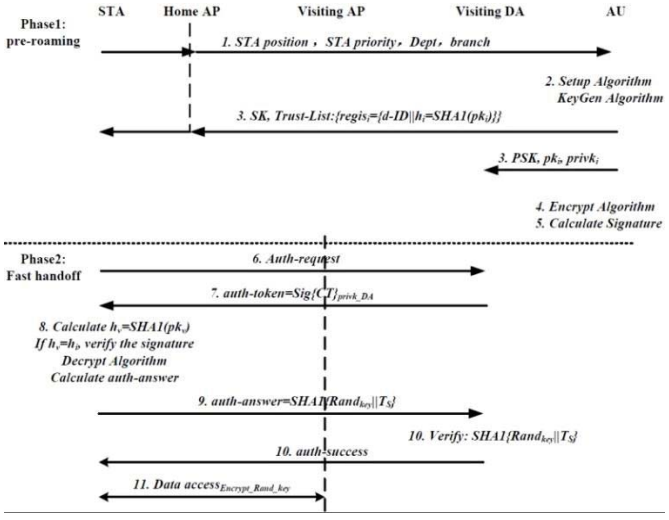

Figure 4. Handoff procedure

Phase 1. Preparation

The purpose of Phase 1 is to make preparation for future roaming.

1. STA sends a message: {*STA position, STA priority*, *dept, branch*} to the trusted authority by using the secure channel established between DA and AU.

2.The trusted authority implements the KeyGen algorithm which takes as input the master key generated by the Setup algorithm and a set of attributes *S*, generates a private key *SK* that identified by that set. The Setup algorithm and KeyGen algorithm are implemented as follow:

Setup: The trusted authority calls the Setup algorithm to create the public key PSK and the master secret key MSK. PSK will be made public to every DA and MSK will be kept secret. Let $\mathbb{G}_0$ be a bilinear group with generator g of prime order p. Next, generate random value$a, b \in \mathbb{Z}_p$. PSK and MSK are generated as follows:

$$\text{PSK} = (\mathbb{G}_0, g, h = g^b, e(g,g)^a) \quad (1)$$

$$\text{MSK} = (b, g^a) \quad (2)$$

KeyGen: The trusted authority generates a private key identified with the attributes set *S* by calling the KeyGen algorithm:

1) generate a random value $n \in \mathbb{Z}_p$;
2) We define the attributes set as *S:{STA position, STA priority*, *dept, branch}*;
3) We also generate each attribute $k \in S$ a random value $n_k \in \mathbb{Z}_p$;
4) Then $SK = (D = g^{(a+n)/b}, \forall k \in S: D_k = g^n \cdot H(k)^{n_k}, D'_k = g^{n_k})$ (3)

3. When the Setup and KeyGen algorithm are completed, the trusted authority sends back the *SK* together with a *Trust-List* to the mobile station as well as makes the *PSK* public to the authenticated domain authenticators.

4. The domain authenticator implements the Encrypt algorithm and generates an *auth- token* as follow:

Encrypt (PSK, Msg, $\mathcal{T}$): The domain authenticator implements the Encrypt algorithm to encrypt a message under the tree access structure$\mathcal{T}$.

We generate two random value $Rand_{key}$, s, and set $q_R(0) = s$, (q_i denotes the value of the polynomial for node *i* of the tree). Let L be the set of leaf nodes, $att(l)$ denote the attribute associated with the leaf node *l* and $\text{Msg} = Rand_{key}$.

The ciphertext *CT* is computed as follows:

$$CT = \{\mathcal{T}, \tilde{C} = Rand_{key} \cdot e(g,g)^{as}, C = h^s, \forall l \in L: C_l = g^{q_l(0)}, C'_l = H(att(l))^{q_l(0)}\} \quad (4)$$

5. The AU signs the ciphertext *CT* by using its private key, and computes its *auth-token* as follows:

$$\textit{auth-token} = \text{Sig}\{\text{CT}\}_{privk\_DA}$$

Phase 2. Roaming

6. When roaming into a visiting domain, the mobile station first sends an *auth-request* to the visiting DA.

7. The DA sends *auth-token* to the STA to start mutual authentication.

8. The STA runs as the following procedure to complete the mutual authentication:

h_v is computed as $\text{h}_v = \text{SHA1}(pk_v)$, where pk_v is the public key of visiting DA. Next, consult the *Trusted-List* for the *regis* information of the visiting domain and authenticate the visiting domain as follows:

1) If $h_v = h_i$, verify the signature. If the signature verification is successful，then the identity of the visiting domain is authenticated.
2) Else if $h_v \neq h_i$ or the signature verification fails, then the identity authentication of the visiting domain is failed.

Decrypt (*CT, SK*): This algorithm implemented by the mobile station accepts ciphertext *CT* and STA's *SK* as input. This algorithm first calls a recursive algorithm DecryptNode to verify whether the tree access structure $\mathcal{T}$ is satisfied by attributes set *S* implicitly contained in the *SK*. If and only if the tree is satisfied by *S*, set *A*=DecryptNode (*CT, SK, R*)= $e(g,g)^{ns}$, we can use *A* to decrypt $\tilde{C}$. The algorithm decrypts by computing

$$Rand_{key} = \tilde{C}/(e(C,D)/A) = \tilde{C}/(e(h^s, g^{\frac{a+n}{b}})/e(g,g)^{ns}) \quad (5)$$

9. The STA returns *auth-answer* to DA which is computed as

$$\textit{auth-answer} = SHA1(Rand_{key}||T_s),\ T_s \textit{ is Timestamp}$$

10. The DA verifies *auth-answer*, then the authentication process is accomplished.

11. Data communication encrypted by $Rand_{key}$.

4 Security analysis

Passive Attack

The *auth-token* during roaming authentication is encrypted using ABE. After the roaming authentication, the traffic is encrypted by using $Rand_{key}$. So there is no information leakage in passive attack.

Bogus Mobile Station

If a mobile station is willing to roam between trusted domains, it must be able to decrypt the *auth-token*. In order to do this, the attacker must have the *SK* which is only assigned to the mobile stations that has performed full authentication in its home domain. For this reason, it is clearly impossible for a bogus mobile station access into a trusted domain in our scheme.

Bogus AP

As we described above that an AP is response for delivering the *auth-token* from the domain authenticator to the roaming mobile station. Since the ciphertext in the *auth-token* should be encrypted using *PSK* which is generated and assigned only to the trusted domain. For that reason, in our scheme, it is obviously ineffective to perform bogus AP attack.

Colluding Attack

The main challenge of our scheme is to prevent against attacks from colluding users. As in the scheme of Sahai and Waters [8, 9], our solution is to randomize users private keys such that they cannot be combined. In order to decrypt the ciphertext *CT*, an attacker clearly must recover $e(g,g)^{as}$. In order to do this the attacker must pair *C* from the ciphertext with the *D* component from some user's private key. This will result in the desired value $e(g,g)^{as}$, but blinded by value $e(g,g)^{ns}$. This value can be blinded out if and only if enough the user has the correct key components to satisfy secret sharing scheme embedded in the ciphertext. Collusion attacks won't help since the blinding value is randomized to the randomness from a particular user's private key.

5 Performance Measurements

In this section we provide an implementation of our scheme by calling the CPABE toolkit to measure the performance of our scheme and see whether it can realize the roaming process fast enough to maintain real time service. We implemented our scheme by using Eclipse JUNO on Ubuntu 12.04 LTSOS. Then we compiled with gcc 4.6.3 and ran the software implementation on a 3.40 GHz Intel Core i3-2130 CPU 32 bits PC with 2 GB RAM.

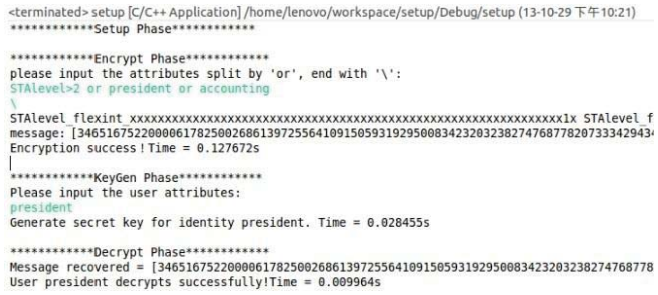

Figure 5. A sample console result

Figure 5 shows the sample console result using our SFCAB scheme. In this sample, the visiting DA encrypt N_k with an access control policy that, 'STA level > 2' or 'president' or 'accounting'. User who has the attribute of 'president' can successfully decrypt.

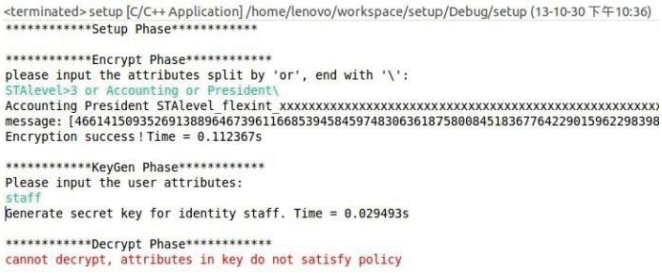

Figure 6. A failure sample console result

Figure 6 shows a failure example. In this example, user with attribute 'staff' tries to decrypt CT from the *auth-token* which is encrypted to 'STA level > 3' or 'Accounting' or 'President'. As shown in Figure 6, this user fails to decrypt.

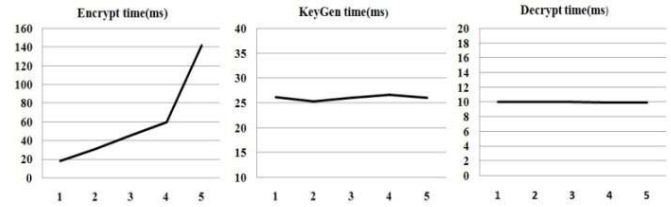

Figure 7. The performance of each algorithm

Measurements of encryption time, key generation time and decryption time produced by running cpabe-setup, cpabe-enc, cpabe-keygen and cpabe-dec are separately displayed Figure 7. Additionally, the performance of each experiment is listed in Table 1.

The performance of cpabe-keygen and cpabe-dec are almost independent of the number of attributes, of which the performance time on average are 26.06ms and 9.98ms, respectively. As shown in figure 7, cpabe-enc run in precisely linear in the number of attributes for the first four points. However, it should be pointed out that the fifth attribute is the only one numerical attribute 'a > 3' in these attributes which is specific that it contains more than one leaf node to represent a numerical attribute in the tree structure.

Table 1. The performance time of each algorithm (ms)

Number of attributes	Encrypt	KeyGen	Decrypt
1	18.1	26.2	10.0
2	30.9	25.3	10.0
3	45.3	26.1	10.0
4	59.6	26.6	9.9
5	142.2	26.1	9.9

6 Conclusion

We propose the first handoff scheme that uses Attribute-based Encryption System to realize security-requirement-oriented access control. Our scheme not only enables the network domains to create their own access policy to but also ensures that only the users satisfy the policy are able to access. Analysis shows that our scheme is fast enough to support real time service in enterprise network.

References

[1] Mercer, Robert A. "Overview of enterprise network developments. "Communications Magazine, IEEE 34.1 (1996): 30-37.

[2] IEEE 802.11 Working Group. "IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements", 2004.

[3] Clancy, T. Charles. "Secure handover in enterprise WLANs: CAPWAP, HOKEY, and IEEE 802.11 r". Wireless Communications, IEEE 15.5 (2008): 80-85.

[4] IEEE 802.11 Working Group. "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirementsPart11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition", 2008.

[5] O'hara, B., and P. Calhoun. J. Kempf, "Configuration and Provisioning for Wireless Access Points (CAPWAP) Problem Statement". RFC 3990, February, 2005.

[6] Kim, Yoohwan, et al. "SFRIC: a secure fast roaming scheme in wireless LAN using ID-based cryptography". Communications, 2007. ICC'07. IEEE International Conference on. IEEE, 2007.

[7] Deng, Yueming, Guojun Wang, and Jiannong Cao. "Trust-Based Fast Inter-Domain Secure Handoff over Heterogeneous Wireless Networks". Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on. IEEE, 2011.

[8] Sahai, Amit, and Brent Waters. “Fuzzy identity-based encryption” .Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005. 457-473.
[9] Bethencourt, John, Amit Sahai, and Brent Waters. “Ciphertext-policy attribute-based encryption”. Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007.
[10] J. Bethencourt, A. Sahai, and B. Waters. “The cpabe toolkit”. http://acsc.csl.sri.com/cpabe/.
[11] B. Lynn. “The Pairing-Based Cryptography (PBC) library”. http://crypto.stanford.edu/pbc.
[12] Tabassam, Ahmad Ali, et al. “Fast and seamless handover for secure mobile industrial applications with 802.11 r”. Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on. IEEE, 2009.