Secure-Positioning-Protocol-Based Symmetric Cryptography

Qingshui Xue
Dept. of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai, China
xue-qsh@sjtu.edu.cn

Fengying Li
School of Continuous Education
Shanghai Jiao Tong University
Shanghai, China
fyli@sjtu.edu.cn

Zhenfu Cao
Dept. of Computer Science and Engineering
Shanghai Jiao Tong University
Shanghai, China
zfcao@cs.sjtu.edu.cn

***Abstract*—Position-based cryptography has attracted lots of researchers' attention. In the mobile Internet, there are lots of position-based security applications. For the first time, one new conception, positioning-protocol-based symmetric cryptography is proposed. Based on one secure positioning protocol, one symmetric model is proposed. In the model, positioning protocols are bound to symmetric cryptography tightly, not loosely. Moreover, we propose one concrete positioning-protocol-based symmetric scheme, its correctness is proved and its security is simply analyzed as well. To our best knowledge, it is the first positioning-protocol-based symmetric scheme.**

Keywords-positioning protocol; symmetric cryptography; UC security; model; scheme

I. INTRODUCTION

In the setting of the mobile Internet, position services and position binding security applications become key requirements, especially the latter. Position services include position inquiring, secure positioning and so on. Position inquiring consists of inquiring your own position and positioning of other entities, which can be realized by TOA/AOA/RMS (radio/light or sound), Camera, Sensor and so forth [1-6]. The technology of inquiring your own position has GPS (Global Positioning System) and so on. The technology of positioning of other entities has Radar and so forth [2-6]. As we all know, the positioning of other entities is a more challenging one. Position binding security applications such as position-based encryption and position-based signature and authentication. For example, when one mobile user sends messages to one specified position which is one either physical or logical address (such as Internet Protocol address), it is desirable that only the user who is indeed at that address can receive it and decrypt messages. If the original receiver at that position because of some reasons leaves that address, it will not be able to receive or decrypt messages any more. In addition, if the original receiver at that place moves to another place, maybe he/she hopes he/she can receive messages at the new place. Take position-based signature and authentication, for example. One mobile or fixed user signs messages at one place and sends them to another mobile user. The receiver can receive the signed message and verify that received messages are really signed at the place by the sender. Even if the signer moves to another address, it will not influence the receiving and verification of signed messages. On March 8 of 2014, the missing Malaysian Airline MH370 can't be found till now, as reminds us of the significance of positioning and related security applications.

Currently, research on position-based cryptography focuses on secure positioning, about which some works had been proposed [1]. These positioning protocols are based on one-dimension, two-dimension or three-dimension spaces, including traditional wireless network settings [1], as well as quantum settings [7-9]. It seems to us that position-based cryptography should integrate secure positioning with cryptographic primitives. If only concentrating on positioning protocols, perhaps we will become far away from position-based cryptography. In other words, nowadays positioning protocols are bound loosely with relevant security applications, not tightly, as results in slow progresses of position-based cryptography and applications. Resorting to the thoughts, in the paper, our main contributions are as follows.

(1) We propose the definition and the model of positioning-protocol-based symmetric cryptography. First, positioning-protocol-based symmetric cryptography is a kind of symmetric one, but a novel one. The definition is given and its model is constructed. We define its security properties as well.

(2) To realize the kind of symmetric cryptography, one secure-positioning-protocol-based symmetric scheme is proposed and its security is analyzed in brief.

In the paper, we will organize the rest as follows. In Section 2, we will introduce the function of positioning protocols and

MOBIHEALTH 2014, November 03-05, Athens, Greece

DOI 10.4108/icst.mobihealth.2014.257200

one secure positioning protocol. In Section 3, one model and the definition of positioning-protocol-based symmetric cryptography are provided. We will propose one positioning-protocol-based symmetric cryptographic scheme in Section 4. Its correctness is proved in Section 5. The security of the proposed scheme will be briefly analyzed in Section 6. Finally, the conclusion is given.

II. POSITIONING PROTOCOLS

In the section, we will introduce the function of positioning protocols and one secure positioning protocol.

A. Function of Positioning Protocols

The goal of positioning protocol is to check whether one position claimer is really at the position claimed by it. Generally speaking, in the positioning protocol, there are at least two participants including position claimers and verifiers, where the verifiers may be regarded as position infrastructure. According to destination of the positioning, there are two kinds of positioning protocol, i.e., your own position positioning protocol and others' position positioning protocol. As of now, lots of work on your own position positioning protocol have been done [2-6]. Nevertheless, research on others' positions positioning protocol is far less and there are still many open questions to resolve. In our model and scheme, we will make full use of the two varieties of positioning protocol.

B. One Secure Positioning Protocol

Here, we will introduce one others' positions positioning protocol. Compared with your own position positioning protocols, others' positions positioning protocols are more complex.

In the section, we will review N. Chandran et al.'s secure positioning protocol in 3-dimension space [1], which can be used in the mobile Internet.

In the protocol, 4 verifiers denoted by $V_1, V_2, ..., V_4$, which can output string X_i, are used. The prover claims his/her position which is enclosed in the tetrahedron defined by the 4 verifiers. Let $t_1, ..., t_4$ be the time taken for radio waves to arrive at the point P from verifier $V_1, V_2, ..., V_4$ respectively. When we say that $V_1, V_2, ..., V_4$ broadcast messages such that they "meet" at P, we mean that they broadcast the messages at time $T - t_1, T - t_2, T - t_3$ and $T - t_4$ respectively so that at time T all the messages are at position P in space. The protocol uses a pseudorandom generator namely an ε-secure $PRG: \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^m$. They select the parameters such that $\varepsilon + 2^{-m}$ is negligible in the security parameters. X_i denotes a string chosen randomly from a reverse block entropy source. The protocol is given as follows:

Step 1. $V_1, ..., V_3$ and V_4 pick keys $K_1, ..., K_3$ and K_4 selected randomly from $\{0,1\}^m$ and broadcast them through their private channel.

Step 2. For the purpose of enabling the device at P to calculate K_i for $1 \le i \le 4$, the verifiers do as follows. V_1 broadcasts key K_1 at time $T - t_1$. V_2 broadcasts X_1 at time $T - t_2$ and meanwhile broadcasts $K_2^{'} = PRG(X_1, K_1) \oplus K_2$. Similarly, at time $T - t_3$, V_3 broadcasts $(X_2, K_3^{'} = PRG(X_2, K_2) \oplus K_3)$, and V_4 broadcasts $(X_3, K_4^{'} = PRG(X_3, K_3) \oplus K_4)$ at time $T - t_4$.

Step 3. At time T, the prover at position P calculates messages $K_{i+1}^{'} = PRG(X_i, K_i) \oplus K_{i+1}$ for $1 \le i \le 3$. Then it sends K_4 to all verifiers.

Step 4. All verifiers check that the string K_4 is received at time $(T + t_i)$ and that it equals K_4 that they pre-picked. If the verifications hold, the position claim of the prover is accepted and it is supposed to be indeed at position P. Otherwise, the position claim is invalid.

III. THE MODEL

A. The model

In the model, there are three parties including Sender, Receiver and Position Infrastructure (for simplicity, called PI). Sender takes responsibility of confirmation of positions of Receiver and encryption of messages sent to Receiver; it should be noted that only if Sender can make sure that Receiver's position is valid before encrypting, he/she can proceed. That's to say, before Sender encrypts messages, even if Receiver is not at that place, as long as the position is Receiver's valid one, it will work. If hoping that Receiver has to be at that position before Sender encrypts, we can construct other models. Receiver is responsible for the confirmation of his or her own position by PI or other self-positioning systems and decryption of ciphertext; PI which is one trusted third party, is used to verify or provide Sender or Receiver's valid positions. The model is depicted in Fig. 1.

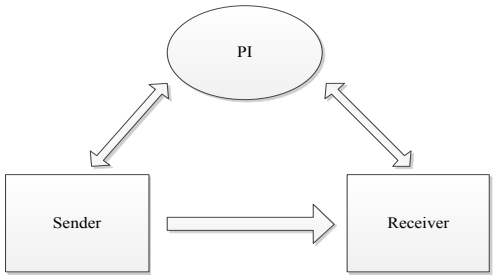

Figure 1. Model of positioning-protocol-based symmetric cryptography

B. Definition

Positioning-protocol-based symmetric cryptography.

Simply speaking, the cryptography combines traditional symmetric cryptography and positioning protocols as one single scheme. It belongs to one-time cryptographic schemes. It is mainly composed of two primitives of sender encryption and receiver decryption. In the course of sender encryption, the sender first confirms the position of the receiver by

This paper is supported by NSFC under Grant No. 61170227, Ministry of Education Fund under Grant No. 14YJA880033, and Shanghai Projects under Grant No. 2013BTQ001, XZ201301 and 2013001.

running positioning protocols and gets the corresponding symmetric key (of course, the receiver also gets the symmetric key, but only during receiver decryption) . By using the symmetric key, the sender encrypts one message and then sends the ciphertext to the receiver. At the side of the receiver, or during the receiver decryption, the receiver first checks its own position by implementing positioning protocols with PI. If its position is valid or right, PI will send the symmetric key to the receiver and the receiver is capable of decrypting the ciphertext; otherwise, the receiver will not be able to gain the corresponding symmetric key to decrypt or reject decrypting the ciphertext.

Remark 1. During the course of sender encryption, if the sender doesn't run the positioning protocol or fails to run the positioning protocol, the session or symmetric key will not be generated by PI and it can't enable the sender to encrypt one message. Similarly, in the course of receiver decryption, if the receiver does not implement positioning protocols to confirm its position, it will not be able to decrypt the ciphertext. From this, it can be seen that the positioning protocol is bound tightly with the generation of symmetric keys, encryption and decryption, instead loosely.

In formulation, the positioning-protocol-based symmetric cryptography consists of three primitives (Initialization, PropEncryption, PropDecryption). Here $h(\bullet$ is one secure hash function.

Initialization. PI takes as input secure parameter 1^k and outputs system master key mk and public parameter pp, meanwhile, the system distributes user identity ID_i for user i. In the model, the primitive or phase can be run only once when setting up the system.

PropEncryption. Sender generates one nonce $n_{sender,PI}$, gets the identity $ID_{receiver}$ and position $Pos_{receiver}$ of the receiver. $Pos_{receiver}$ is from PI and is Receiver's valid position. Meanwhile, the sender will receive another nonce $n_{PI,receiver}$ from PI, the sender will generate one-time session or symmetric key by $sk = h(n_{sender,PI}, n_{PI,receiver})$. Sender encrypts message m by any symmetric cryptographic algorithm such as AES using session key sk, and c is the corresponding ciphertext. The ciphertext is $(n_{sender,PI}, c)$ and is sent to the receiver.

PropDecryption. After Receiver receives the ciphertext $(n_{sender,PI}, c)$, he/she takes as input the identity $ID_{receiver}$ and position $Pos_{receiver}$ of Receiver to run the positioning protocol with PI. If the receiver is indeed at the position, PI sends the nonce $n_{PI,receiver}$ which was used during the PropEncryption to the receiver. Otherwise, the receiver can't get the nonce $n_{PI,receiver}$. From the ciphertext $(n_{sender,PI}, c)$ from the sender and the nonce $n_{PI,receiver}$, the receiver can recover the session key by $sk = h(n_{sender,PI}, n_{PI,receiver})$. Then the receiver can decrypt the ciphertext $(n_{sender,PI}, c)$ and gets the plaintext m.

The formulation is illustrated Fig. 2.

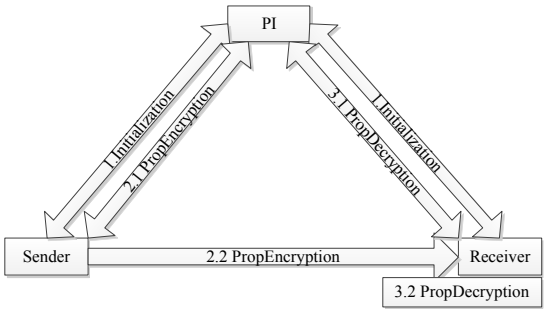

Figure 2. Formulation of positioning-protocol-based symmetric cryptography

C. *Security Properties of Positioning-Protocol-Based Symmetric Cryptography*

(1) Positioning protocol binding. In the course of PropEncryption, the sender is requested to confirm the position of the receiver by communicating with PI. During the course of PropDecryption, the receiver has to confirm its own position by PI. That is to say, although the receiver is at the right position, if it does not confirm its position by PI, it will not be able to get the nonce which is generated by PI during the course of PropEncryption, as means that it can't get the session key. Because the model is of one–time cryptography, after it receivers the ciphertext, if it moves from its original position to another one, its position confirmation by PI will not succeed, it is unable to get the session key to decrypt the ciphertext.

Remark 2. In our model, we use one-time encryption. Why do we do so? In position-based encryption schemes, if the receiver of ciphertext moves to another place, rather than its original one, it can still decrypt received other ciphertexts when not using one-time encryption. That's to say, in position-based encryption schemes, to decrypt the ciphertext, only session or symmetric keys can't work. It needs other information such as position authentication and positioning to cooperate. This tells us one basic fact that encrypting keys of position-based encryption or the signing keys of position-based digital signature should not be fixed, at least multiple, or random (one-time keys).

IV. ONE SECURE-POSITIONING-PROTOCOL-BASED SYMMETRIC SCHEME

As the above model does, there are mainly three participants: Sender, Receiver and PI. In addition, PI will play the role of system authority. In the scheme, there are three phases: Initialization phase, PropEncryption phase and PropDecryption phase. In the scheme, when confirming of other parties' positions, the secure positioning protocol [1] mentioned above can be used. When verifying one participant's own position, GPS or other technologies can be used. So, here the secure positioning protocol and GPS play the role of PI.

A. Initialization

PI takes as input secure parameter 1^k and outputs system master key mk and public parameter pp, meanwhile the system distributes user identity ID_i for user i.

B. PropEncryption

Sender generates one nonce $n_{sender,PI}$, gets the identity $ID_{receiver}$ and position $Pos_{receiver}$ of the receiver. $Pos_{receiver}$ is from PI and is receiver's valid position. Meanwhile, Sender receives one nonce $n_{PI,receiver}$ from PI, then Sender generates one-time session key by $sk = h(n_{sender,PI}, n_{PI,receiver}, Pos_{receiver}, ID_{receiver})$. Sender encrypts the message m by any symmetric cryptographic algorithm using session key sk, and c is the corresponding ciphertext. The ciphertext is $(n_{sender,PI}, c)$ and is sent to Receiver.

C. PropDecryption

Receiver takes as input the identity $ID_{receiver}$ and position $Pos_{receiver}$ of its own to run the positioning protocol with PI. If Receiver is indeed at the position, PI sends the nonce $n_{PI,receiver}$ which was used during the PropEncryption to Receiver. Otherwise, the receiver can't get the nonce $n_{PI,receiver}$. From the ciphertext $(n_{sender,PI}, c)$ from the sender and the nonce $n_{PI,receiver}$ from PI, Receiver can recover the session key by $sk = h(n_{sender,PI}, n_{PI,receiver}, Pos_{receiver}, ID_{receiver})$. Then the receiver can decrypt the ciphertext $(n_{sender,PI}, c)$ and get the plaintext m.

V. Correctness of the Above Scheme

About the correctness of the above scheme, we have the following theorem.

Theorem 1: If the scheme correctly runs according to the above phases, Receiver can share the session key or symmetric key with Sender to decrypt the ciphertext.

Proof.

In the course of PropEncryption, Sender generates the nonce $n_{sender,PI}$, gets the identity $ID_{receiver}$ and position $Pos_{receiver}$ of Receiver, and receives the nonce $n_{PI,receiver}$ from PI, Sender can produce one-time session key by $sk = h(n_{sender,PI}, n_{PI,receiver}, Pos_{receiver}, ID_{receiver})$. In the course of PropDecryption, from the ciphertext $(n_{sender,PI}, c)$, the receiver can get $n_{sender,PI}$. From PI, the receiver can get $n_{PI,receiver}$, if and only if its position is confirmed to be truly $Pos_{receiver}$. Because Receiver has the knowledge of its identity and position, it can compute the session key $sk = h(n_{sender,PI}, n_{PI,receiver}, Pos_{receiver}, ID_{receiver})$. Thus, Receiver and Sender can get and share the one-time session key $sk = h(n_{sender,PI}, n_{PI,receiver}, Pos_{receiver}, ID_{receiver})$. It is proved.

□

VI. Security Analysis of the Above Scheme

In the proposed scheme, we make use of four kinds of technology, i.e. one-time symmetric/session key, secure positioning protocols including others' positions positioning and your own position positioning, symmetric encryption and certificates. That is to say, the security of the proposed scheme relies on the security of the used three kinds of technology. Because the proposed scheme or the model is one composition framework, it is appropriate that its security is analyzed from the UC (Universal Composition) framework [10]. We will detail its security analysis in its full version.

VII. Conclusions

In the paper, according to security requirements of the mobile Internet, we construct a positioning-protocol-based symmetric encryption model. Its definition and security properties are given. As far as we know, it is the first model combining positioning protocol and symmetric encryption. Meanwhile, we also propose one positioning-protocol-based symmetric scheme and analyze its security. We will further perfect relevant models and schemes, as well as positioning-protocol-based asymmetric encryption and positioning-protocol-based signature. It is believed by us that the research on positioning-protocol-based cryptographic models or schemes in the mobile Internet will become one focus.

References

[1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position Based Cryptography," CRYPTO 2009, pp. 391-407.

[2] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," WiSe '03-Proceedings of the 2003 ACM workshop on Wireless security, 2003, pp.1-10.

[3] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," IEEE Conference on Mobile Adhoc and Sensor Systems Conference, 2005.

[4] L. Bussard, Trust Establishment Protocols for Communicating Devices, PhD thesis, Eurecom-ENST, 2004.

[5] S. Capkun and J. P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," IEEE INFOCOM, 2005, pp.1917-1928.

[6] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations." IEEE INFOCOM, 2006.

[7] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-Based Quantum Cryptography: Impossibility and Constructions," CRYPTO 2011, pp. 429-446.

[8] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, "Position-Based Quantum Cryptography: Impossibility and Constructions," CoRR abs/1009.2490, 2010.

[9] H. Buhrman, S. Fehr, C. Schaffner, and F. Speelman, "The Garden-Hose Game: A New Model of Computation, and Application to Position-Based Quantum Cryptography," CoRR abs/1109.2563, 2011.

[10] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," http://eprint. iacr.org/2000/067, 2000.