Enhancement to the Privacy-aware Authentication for Wi-Fi based Indoor Positioning Systems

Jhonattan J. Barriga A. [1,2] [0000-0001-7334-9113], Sang Guun Yoo [1,2,*] [0000-0003-1376-3843] and Juan Carlos Polo [3]

[1] Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito, Ecuador, [jhonattan.barriga,sang.yoo]@epn.edu.ec

[2] Smart Lab, Escuela Politécnica Nacional, Quito, Ecuador

[3] Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE, Sangolqui, Ecuador, jcpolo@espe.edu.ec

[*] Corresponding author: sang.yoo@epn.edu.ec

Abstract. Indoor location-based application and services based on Wi-Fi have serious problems in terms of privacy since attackers could track users by capturing their MAC addresses. Although several initiatives have been proposed by scientific community to properly address authentication by strongly preserving privacy, there are still improvements and steps that need to be developed as it is not clearly stated what would occur if a device is lost, stole or compromised. It has not been said how an affected user should proceed in such case. In this situation, this work provides an enhancement to a previous solution based on pseudo-certificates issued by third-party authorities for anonymous auhentication of mobile devices. The proposed scheme provides privacy to users willing to remove a device that has been stolen or lost. The proposed system offers security while maintaining minimal cryptographic overhead.

Keywords: Privacy, Anonymous de-authentication, Indoor positioning system, IPS, WLAN

1 Introduction

Scientific community and industry show a great interest on improving the accuracy of Indoor Positioning Systems (IPS) [1]–[3] because it is an alternative to GPS and it could be applied to different areas of Internet of Things such as healthcare and social life [2], [4]. Even though several technologies could be applied to acquire indoor positioning data, Wi-Fi is the most used technology since it is widely used among private and public organizations [3], [5].

Different improvements of indoor positioning systems have been presented in different works; however, in most of cases, the privacy issue has been left aside [6], [7]. Similarly, a novel privacy-aware authentication system for Wi-Fi IPS was proposed in

adfa, p. 1, 2011.

[8]. Likewise, there are other approaches looking for protecting the privacy of users based on lightweight solutions [9], Secure Two Party Communication (STPC) [10], Physical Signatures [11] or application to change MAC address randomly [12]. Additionally, there are other solutions that use continuous authentication with the exclusion of identifiers from message headers [13] or propose an scheme based on a secret, token and biometrics [14]. As shown, many solutions have been proposed to perform authentication by preserving anonymity. However, the aforementioned related works, in spite of being secure and privacy conservatives, do not consider the whole scenario which is associated when a device has been lost, stolen or compromised and needs to be removed from the system. The user must have the power to perform such action as he/she is the owner of the device. Moreover, the intervention of a system administrator would cause more problems since the administrator could unsubscribe a valid user by mistake or since the user will have to follow an administrative procedure to request the device removal making the user to wait longer than expected.

The use of pseudo-certificates guarantees privacy because they do not store users' information and they have a validity time to prevent being reused after a certain period of time [8]. However, such security mechanism is not enough since if a malicious user manages to obtain a valid (loss or stolen) device, he/she will be able to access to the system as the device is a registered equipment with a valid set of credentials. For this reason, this paper intends to make an improvement of [8] by providing a simple but secure mechanism for users with valid credentials that allows users removing their devices from the system. To reach this goal, it is necessary to design a proper protocol with features that allow to remove every record of the device from the whole system without disclosing information and preserving privacy and anonymity. In summary, the major contribution of this paper is to enhance a protocol designed in a previous work [8] by proposing a novel initiative to securely remove a device of a particular individual that was previously registered in the system [3], [15]

The rest of the paper is structured as follows, section 2 comprises a brief revision on authentication protocols for indoor positioning systems based on WLAN. Then, the proposed solution is explained with details in section 3. Later, section 4 analyzes the proposed solution in terms of security and performance. Finally, the paper is concluded in section 5.

2 State of the Art

Scientific community has focused on addressing privacy issues by proposing different works [8]–[17]. Reference [5] discusses several of those proposals including solutions based on obfuscation of sensitive data and usage of random MAC addresses. In [13] a proximity based control is proposed where the authors emphasize on removing previously generated information over packets to preserve privacy. An approach focused on a triple combination of a token, secret and biometrics is discussed in [14]. Such work is mainly oriented to use a smart phone to authenticate and authorize over a location-

based system; in such system, two protocols are proposed: one for registration and another to handle authorization and authentication. Although the solution addresses privacy and authentication in a secure way, it does not describe how to remove a device that has been lost or stolen i.e. compromised. Likewise, the reference [10] indicates that the IPS server could violates user's privacy and that the device could forces the system to disclose its location. Their solution suggests the use of a Secure Two-Party Computation (STP) to protect the privacy of all the involved participants. In this approach, the user encrypts and sends the private inputs (RSSI distance measured from APs) to the server with a secure algorithm. However, this approach does not deliver an authentication mechanism before attaching to the system which means that any user would be able to send his/her inputs. Additionally, in case that a user wanted to be removed from the system, there is no formal process to achieve such goal. Indeed, lack of authentication might lead that the user would send its position to a rogue IPS server that might be deployed within the same network.

Moreover, the proposal discussed in [16] presents an algorithm called *TemporalVectorMap* (TVM). It allows a user to accurately know his/her position by taking advantage of a k-Anonymity Bloom (*kAB*) filter and a *bestNeighbors* generator of camouflaged localization requests. According to the authors, both of the aforementioned techniques seem to be resilient to some privacy attacks. This proposal draws two phases: (i) initial localization and (ii) continuous localization. During the first phase, the *kAB* is built based on the MAC address of an Access Point (AP), assuming that the AP is valid within the context of the network as it has been registered by the server. Phase of continuous location implements *bestNeighbors* algorithms to handle users that could be moving around the deployed ecosystem. Authors suggests that their solution is not prone to linking attack as there are no attribute records stored in the server and it is resistant to homogeneity attack as it uses hashing to generate a set of unique AP MAC values. Anyhow, along this solution, there is no formal procedure for registering or removing a device.

Another approach based on WLAN for wireless sensor networks is discussed in [9]. The authors propose a lightweight authentication protocol which is mainly based on Fermat Number Transform (FNT) and Chinese Remainder Theorem (CRT) to maintain secure communication. The encryption and decryption algorithm are based on a protocol that involves a combination of substitution cipher and columnar transposition which withstands linear crypt analysis rather than using a formal known one. The authentication relies on generating a prime number that is stored in the node and in the server. The node sends an authentication request to the server which is processed and validated at the base station. Although this schema considers a secure authentication schema, it does not deliver an optimal process for compromised node removal since the administrator has to remove the compromised node's key from the base station.

Furthermore, the solution named as "IMAKA-Tate" [17] proposes an schema based on three-way handshake mutual authentication and key agreement in conjunction with authentication against an Extensible Authentication Protocol (EAP). Mutual Authentication and Key Agreement are used so that each participant generates random challenge, which is encrypted by the corresponding public key of the recipient. This work

properly addresses anonymity and privacy, but it does not include a formal procedure for device removal.

The solution discussed in [11] proposes an authentication protocol IPS based in WLAN that verifies user information based on the physical layer (PHY) signatures within WLAN preambles. It mainly uses Carrier Frequency Offset (CFO) and multipath plus Channel State Information (CSI) to protect wireless communications since the handshake phase between the mobile users and the access point (AP), and whilst validating the truthfulness of a reported location from a user of the system. In this current solution, there is no need of credentials for registering the user as everything is handled at the PHY layer. This solution, like the previous ones, lacks from having a formal procedure to remove an undesired device from the system (remove from authentication system).

A privacy protection mechanism for indoor positioning is presented in [12]. This mechanism proposes the use of an application that changes the MAC address of the phone periodically. They use this approach to provide privacy to the user as the server will not determine his/her identity. Although privacy is protected, there might be a potential issue if a MAC address is repeated along two users handling the same manufacturer phone. The process of authentication is not formally defined, but it appears that the application installed will be in charge on performing such action. Again, this solution, like the previous ones, does not deliver a formal process to remove the device from the system rather than uninstalling the application from the phone.

Weaknesses about PriWFL are exploited and discussed in [18]. These weaknesses might let attackers to obtain the position of a user. The authors present a practical Server Data Privacy Attack where they point that an attacker only needs to obtain a pair of distances. They also discuss an attack that reveals the order of RSS values. As stated by the authors there are non-trivial problems that may dramatically affect the localization accuracy. Furthermore, the authors propose Fully Homomorphic Encryption and Somewhat Homomorphic Encryption but they are computational costly or impractical for Wi-Fi schema. Secure Multiparty Computation (MPC) is analyzed but as reviewed by the authors it may generate communication overhead. Paillier PKE is analyzed from two perspectives (Signs of Differences and Garbled Circuits), where the first approach seems secure but might be susceptible to order attack, whilst the second approach is more secure as it resilient to Client Privacy Attacks (scenarios 1 and 2) as the attacker could not infer the location of a client if the secret key is not known. Likewise, if the MPC is secure and the randomness are fresh, an attacker cannot learn combined distances. The inclusion of Paillier encryption let a client to learn only signs of distances. The solution proposed clearly analyze and exploit weaknesses focusing on an attacker compromising the database of a provider. This paper makes good points on preserving privacy.

Practical Privacy-Preserving Indoor Localization using OuTsourcing (PILOT) is another approach which focuses like the previous work on preserving privacy in an Indoor Positioning System [19]. Semi Trusted Third Parties (STTPs), a client and an Indoor Location Provider (ILP) are involved in the approach described by the authors. In the described scenario the client collects signal strengths from access points predefined by the ILP and then shared to the STTPs by a secure channel. Every STTP calculates an

ILP protocol by using a Secure Two-Party Computation (STPC). The solution proposed is secure against semi-honest non-colluding STTPs, malicious clients and ILP servers. According to the authors, the use of the ABY-Framework ensures that intermediate secret-shares are secure as well as conversions, and final target location. The proposed schema guarantees that if one STTP and the client are not compromised; then, the client will not be able to determine its location. Likewise, if the ILP and one STTP are not corrupted and no matter if there is a leak of information, it will not be possible to determine the RSSs of the database of the ILP server. In regards of connectivity this approach relies on secure communication. The main contribution of this paper is a protocol that deals with most of communication and computation on third-parties (STTPs) rather than the mobile client as it poses limited hardware resources. Although this contribution shows a strong on privacy-preserving schema, it does not present as a use case where a device has been compromised or stolen and the user would have the power to act in such case.

Another solution is discussed in [8], where the use of pseudo-certificates helps to provide privacy and anonymity to the user attached to the system. In this proposal, the user first has to register his device, and then the system will generate a set of pseudo-certificates with an expiry time. These certificates will let a server to determine a user position without knowing/revealing its identity. Although this approach describes the process of authentication, it does not handle the process of removing a device.

We have examined several solutions in regards of authentication procedures for IPS based on WLAN. All of them showed the need to have a formal and secure process for removing devices that have been lost or stolen. With this antecedent, our proposal is to perform and enhancement to [8], by adding a formal and secure process for removing devices, giving the user the right to perform such action without compromising his/her privacy. The proposed protocol will be described in detail and analyzed from a security and performance perspectives in the next sections.

3 Proposed Protocol

3.1 Overview of the System

Since the objective of this work is to deliver the mobile device removal process to a previous work, the proposed mechanism uses the same three main entities for Authentication, Authority and Accounting (AAA). A brief overview of the previous work that will be enhanced is shown below (see **Fig. 1**). The reviewed system is composed by three main entities:

1) User environment composed of the user and his/her mobile device(s).

2) A Certificate Authority (CA) which manages the accounts of users, data of their mobile devices, and devices' pseudo-certificates/private keys.

3) An IPS Server that provides the indoor positioning service, which is registered in the CA.

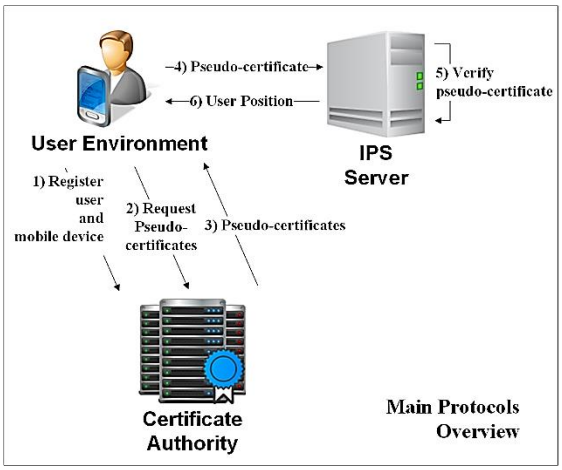

Fig. 1. Overview of the system

For a better understanding of the system, we recommend to refer to the previous work [8].

3.2 Proposal of Device Removal Functionality: An Overview

In a previous work [8], a protocol for providing privacy by using an anonymous authentication schema was designed. However, it does not have a process to remove a previously registered mobile device, which means that a lost or stolen mobile device can be used by an illegal/malicious user. In this sense, this work enhances the previous work by adding the mobile device removal process which contains the following steps (see **Fig. 2**).

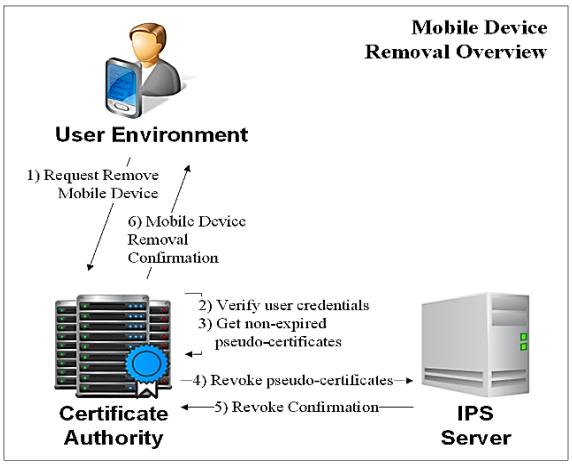

Fig. 2. Proposed enhancement schema

The user who wants to remove his/her device must be previously registered to the Certificate Authority (CA). The user first authenticates using his/her credentials. The CA validates credentials and if successful, it returns a list of available devices registered by such user. The user selects the devices to be removed and submits a request to remove the mobile device. Then, the CA will get all non-expired pseudo-certificates and will perform a request for revoking the pseudo-certificates from the Indoor Positioning System (IPS) Server. For this, the CA sends a list of certificates that need to be revoked by the IPS Server and the IPS server validates the request's authenticity, revokes the pseudo-certificates and confirms the revocation procedure to the CA. Then, the CA removes all the pseudo-certificates associated to the device that needs to be removed. Finally, the user receives a removal confirmation message.

3.3 Proposal of Device Removal Functionality: Details

In the previous subsection, we have described briefly the flow of the proposed system. Now, this subsection will describe the details of the proposed functionality. The notation used to describe the protocol is detailed in **Table 1**.

Table 1. Notations used in the Proposed Solution

Notation	**Description**
U_i	i^{th} user
MD_{i_Ui}	U_i's j^{th} mobile device
RN1, RN2, …, RNn	Random nonces
RK1, RK2... RKn, RK_{CA}, RK_{IPS}	Random symmetric keys
CA	Certificate Authority
$Pubkey_{CA}$, $Prikey_{CA}$	*CA*'s asymmetric key pair
$Pubkey_{IPS}$, $Prikey_{IPS}$	*IPS Server*'s asymmetric key pair
ID_{Ui}	Identification of U_i
PW_{Ui}	Password of U_i
$NAME_{MDj\_Ui}$	Name of MD_{j_Ui}
MAC_{MDj_Ui}	MAC address of MD_{j_Ui}
$\{PCert_{(CA,MDj\_Ui)1}, ..., PCert_{(CA,MDj\_Ui)n}\}$	Pseudo-certificates of MD_{j_Ui}
$\{Prikey_{(CA,MDj\_Ui)1}, ..., Prikey_{(CA,MDj\_Ui)n}\}$	Private keys of pseudo-certificates of MD_{i_Ui}
IP_{IPS}	*IPS Server*'s IP address
$PCert_{(CA,MDj\_Ui)k}$	k^{th} (unused) pseudo-certificate
Pos_{MDj_Ui}	Current position of MD_{j_Ui}
||	String concatenation
h(.)	One-way hash function
AEnc(x,y)	Asymmetric encryption of message *y* using the key *x*
ADec(x,y)	Asymmetric decryption of message *y* using the key *x*
SEnc(x,y)	Symmetric encryption of message *y* using the key *x*
SDec(x,y)	Symmetric decryption of message *y* using the key *x*
Sign(x, y)	Digital signature of message *y* using the private key *x*
VerifySign(x,y)	Digital signature verification of signature *y* using public key *x*

Mobile Device Removal. This protocol is executed as follows (see **Fig. 3**). First, the user U_i inputs his/her identity ID_{Ui} and password PW_{Ui} to his/her mobile device MD_{j_Ui}. Then, MD_{j_Ui} communicates with the third-party *CA* and asks for user authentication. After receiving the request message, *CA* generates a random number *RN8* and sends it to MD_{j_Ui}. Once received the response from *CA*, MD_{i_Ui} generates a random nonce *RN9*, a random symmetric key *RK4*, and calculates $M12=AEnc(Pubkey_{CA}, RK4)$ and $M13=SEnc(RK4, RN8||RN9||ID_{Ui}||h(PW_{Ui}))$, where $AEnc(x,y)$ is an asymmetric encryption of message *y* using the key *x*, $Pubkey_{CA}$ is *CA*'s public key, $SEnc(x,y)$ is a symmetric encryption of message *y* using the key *x*, || is a concatenation operation, and $h(.)$ is a one-way hash function. Once calculated *M12* and *M13*, MD_{j_Ui} sends those values to *CA*.

On the other side, *CA* gets *RK4* by executing $ADec(Prikey_{CA}, M12)$ where $ADec(x,y)$ is an asymmetric decryption of an encrypted message *y* using the key *x*, and uses *RK4* to get *RN8'*, *RN9'*, ID_{Ui}, and $h(PW_{Ui})$ by executing $SDec(RK4, M13)$, where $SDec(x,y)$ is a symmetric decryption of an encrypted message *y* using the key *x*. Once gotten *RN8'*, *CA* verifies the freshness of the message by comparing the decrypted *RN8'* with the random nonce created previously by itself i.e. *RN8*. This step allows *CA* to protect against replay attacks. After verifying the validity of the message, *CA* verifies if ID_{Ui} and $h(PW_{Ui})$ are valid credentials otherwise the process is aborted. If credentials are valid, the CA retrieves a list of registered devices from DB that belong to the user ID_{Ui}, this list is a collection of tuples formed by the *NAME* of the device and its *MAC Address* $\{(NAME_{MD1\_Ui}, MAC_{MDn\_Ui}),\ldots,(NAME_{MDn\_Ui}, MAC_{MDn\_Ui})\}$. Then, the CA generates a random nonce *RN10*, and calculates $M14=SEnc(RK4, RN9'||RN10||\{(NAME_{MD1\_Ui}, MAC_{MDn\_Ui}),\ldots,(NAME_{MD1\_Ui}, MAC_{MDn\_Ui})\})$, which is sent to the mobile device MD_{j_Ui}.

The mobile device MD_{j_Ui} gets $RN9''||RN10||\{(NAME_{MD1\_Ui}, MAC_{MDn\_Ui}),\ldots,(NAME_{MD1\_Ui}, MAC_{MDn\_Ui})\}$ by excecuting $SDec(RK4, M14)$. Once gotten *RN9''*, the mobile device verifies the freshness of the message by comparing the decrypted *RN9''* with the random nonce generated previously by itself i.e. *RN9*. After verifying the authenticity of the message, the mobile device generates $M15 = \{(NAME_{MD1\_Ui}, MAC_{MD1\_Ui}),\ldots,(NAME_{MDn\_Ui}, MAC_{MDn\_Ui})\}$, and display the list of registered devices to the user.

The user U_i selects the registered device from the list (*M15*) that wants be removed (MAC_{MDg_Ui}). The mobile device generates a random nonce *RN11*, and calculates $M16=SEnc(RK4, RN10'||RN11||MAC_{MDg\_Ui})$, and sends *M16* to the CA.

The CA gets $RN10''||RN11||MAC_{MDg\_Ui}$ by executing $SDec(RK4, M16)$. Once gotten *RN10''*, the CA verifies the freshness of the message by comparing the decrypted *RN10''* with the random nonce created before by itself i.e. *RN10*. If such values are the same, the CA gets all the not expired pseudo-certificates of the mobile device that are stored in the DB $\{PCert_{(CA,MDj\_Ui)1}, ..., PCert_{(CA,MDj\_Ui)n}\}$. Then, the CA submits a request to the IPS Server and it generates a random nonce *RN12* which is sent back to the CA. The CA, generates and random nonce *RN13*, a random key RK_{CA} and calculates *M17* and

M18, where $M17=AEnc(PubKey_{IPS},RK_{CA})$. $M18 = SEnc\ (RK_{CA}, RN12 \mid\mid RN13 \mid\mid \{PCert_{(CA,MDj\_Ui)1}, ..., PCert_{(CA,MDj\_Ui)n}\} \mid\mid Sign(PriKey_{CA}, RK_{CA}))$, and $Sign(x,y)$ is the signing function of a message *y* using the private key *x*. Once calcultated *M17* and *M18*, the CA sends those messages to the *IPS Server*.

On the other side, the *IPS Server* gets RK_{CA} by executing $ADec(PriKey_{IPS}, M17)$ and uses it to get $RN12''||RN13'||\{PCert_{(CA,MDj\_Ui)1}, ..., PCert_{(CA,MDj\_Ui)n}\}||Sign(PriKey_{CA}, RK_{CA}))$ by executing $SDec(RK_{CA}, M18)$. Once gotten *RN12''*, the *IPS Server* verifies the freshness of the message by comparing the decrypted *RN12''* with the previously generated random nonce created by itself i.e. *RN12*. After verifying the validity of the message, the *IPS Server* uses $PubKey_{CA}$ to verify the digital signature of the message by executing $VerifySign(PubKey_{CA}, Sign(PriKey_{CA}, RK_{CA}))$ to ensure the authenticity of the message. Once verified the authenticity of the message, the non-expired pseudo-certificates of the registered device $\{PCert_{(CA,MDj\_Ui)1}, ..., PCert_{(CA,MDj\_Ui)n}\}$, are revoked which means that are removed from the DB. Finally, the *IPS Server*, sends *RN13'* to the CA.

Meanwhile, the CA, gets *RN13'* and verifies the freshness of the message by comparing the received *RN13'* with the previously generated random nonce created by itself i.e. *RN13*. After validating the message, the CA removes $NAME_{MDj\_Ui}$, MAC_{MDj_Ui}, $\{PCert_{(CA,MDj\_Ui)1}, ..., PCert_{(CA,MDj\_Ui)n}\}$, and $\{Prikey_{(CA,MDj\_Ui)1}, ..., Prikey_{(CA,MDj\_Ui)n}\}$ corresponding to the previously selected device to be removed (MAC_{MDg_Ui}.). The CA, sents *RN11'* to the user mobile device.

Finally, MD_{j_Ui}, once received *RN11'* from CA, compares such value with the random nonce generated previously by itself i.e. *RN11*. If such values are the same, MD_{j_Ui}, confirms U_i the successful removal of the selected device.

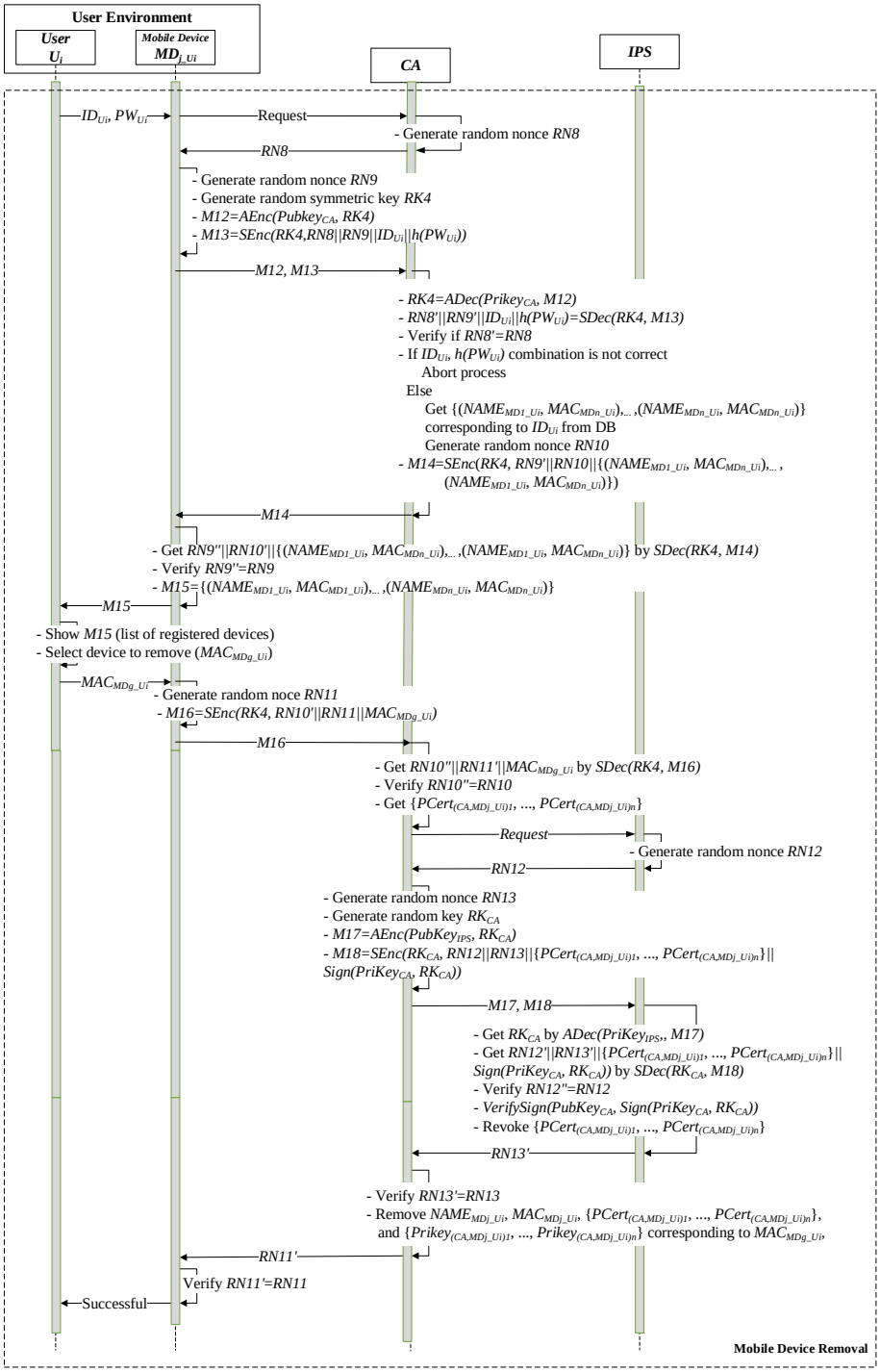

Fig. 3. Mobile Device Removal Protocol

4 Analysis of the Proposed Protocol

This section analyzes the proposed protocol in terms of security and performance in order to evaluate the effectiveness of the protocol from a theoretical perspective.

4.1 Security Analysis

This part examines the security of the proposed protocol in terms of analysis of possible attacks. For this, the widely known Dolev-Yao [20] threat model was used, which assumes that two communicating parties use an insecure channel.

Man in the middle attack. This attack is not possible because the messages are encrypted using secure encryption functions. When MD_{j_Ui} communicates with *CA*, the message is encrypted using the public key of *CA*; when *CA* communicates with MD_{j_Ui} the message is encrypted with the random symmetric key generated by MD_{j_U}; and when CA communicates with *IPS Server* the message is encrypted with the public key of $Pub\text{-}Key_{IPS}$. The usage of secure encryption functions allows proposed protocols to maintain the confidentiality and integrity of messages.

Replay Attack. Random nonces are used to avoid replay attacks in mobile device removal process. On the other hand, an illegal user will not be able to remove a device because the MAC_{MDg_Ui} identifier is symmetrically encrypted.

Password Guessing Attack. PW_{Ui} is not stored anywhere. Instead, a variant value $h(PW_{Ui})$ is used for user validation. Since $h(.)$ is a secure one-way hash function, the attacker cannot guess the PW_{Ui} from $h(PW_{Ui})$. Hence, this attack is not possible.

Privileged-Insider Attack. In the proposed solution, MD_{j_Ui} never transmits the password of the user PW_{Ui} in plaintext. Instead, a variant value $h(PW_{Ui})$ is sent to the *CA*. Even a privileged-insider of CA cannot guess the PW_{Ui} because $h(PW_{Ui})$ is calculated using a secure one-way hash function. Also, a malicious user might try to revoke certificates from a valid device; however, such malicious user will have to manually generate requests to the *IPS Server* to obtain approval for a complete removal.

Brute Force Attack. The attacker can attempt to remove a valid device by sending random or sequential messages to the CA. However, the use of random nonces helps to prevent this attack.

Separation of Responsibilities. *CA* manages only the information of the users/mobile devices while *IPS Server* manages only the information about the relation between a pseudo-certificate and position.

4.2 Performance Analysis

Table 2 indicates the overhead of cryptographic steps of the proposed protocol. It is important to mention that the cryptographic overhead in each protocol is minimal; therefore, it does not affect to the real implementation of the proposed solution.

Table 2. Cryptographic Overhead (i.e. number of operations)

Phase	Entity	Proposed
Mobile Device Removal	$MD_{i\ Ui}$	*1 AEnc + 2 SEnc + 1 H + 1 SDec*
	CA	*2 SEnc + 1 ADec +1 SDec + 1 AEnc + 1 Sign*
	IPS Server	*1 ADec + 1 SDec + 1 VerifySign*

AEnc: Asymmetric encryption, *ADec*: Asymetric decryption, *H*: hash, *SEnc*: Symmetric encryption, *SDec*: Symmetric decryption, *Sign*: Creation of digital signature, *VerifySign*: Verification of digital signature

5 Conclusions and Future Direction

This paper has proposed an enhancement to the novel authentication system for Indoor Positioning Systems that includes a protocol for removing mobile devices. The proposed solution allows a user to remove his/her registered devices if they have been stolen or lost, so that an illegal user will not be able to use it. The proposed solution still provides a secure authentication system for IPS while maintaining a minimal performance overhead. The proposed approach gives to the user the power to securely remove his/her device without the intervention of a third-party, reducing the risk of involuntary mistakes. In the near future, we will continue our research by implementing the suggested protocol in a real scenario and extending to more IoT devices.

6 Acknowledgements

The authors gratefully acknowledge the financial support provided by the Escuela Politécnica Nacional, for the development of the project PIJ-17-08 – "Diseño e Implementación de un Sistema de Parqueadero Inteligente".

7 References

[1] Z. Farid, R. Nordin, and M. Ismail, "Recent Advances in Wireless Indoor Localization Techniques and System," vol. 2013, 2013.

[2] S. He and S. H. G. Chan, "Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 466–490, 2016.

[3] D. H. Stojanović and N. M. Stojanović, "INDOOR LOCALIZATION AND TRACKING : METHODS , TECHNOLOGIES AND RESEARCH CHALLENGES ," vol. 13, no. Iii 43007, pp. 57–72, 2014.

[4] Z. Deng, Y. Yu, X. Yuan, N. Wan, and L. Yang, "Situation and development tendency of indoor positioning," *China Commun.*, vol. 10, no. 3, pp. 42–55, 2013.

[5] E. Lohan, R. P. Examiners, F. Council, and E. Engineering, "User Privacy Risks and Protection in Wlan-Based," 2015.

[6] D. Mendez, I. Papapanagiotou, and B. Yang, "Internet of Things : Survey on Security and Privacy," *Inf. Secur. J. A Glob. Perspect.*, pp. 1–16, 2017.

[7] L. Chen *et al.*, "Robustness , Security and Privacy in Location-Based Services for Future IoT : A Survey," 2017, vol. 5.

[8] S. G. Yoo and J. J. Barriga, "Privacy-Aware Authentication for Wi-Fi Based Indoor

Positioning Systems," in *ATIS 2017*, 2017, no. October, pp. 201–213.

[9] M. D. Shah and S. N. Gala, "Lightweight authentication protocol used in wireless sensor network," in *2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA) Lightweight*, 2014, pp. 138–143.

[10] J. H. Ziegeldorf, N. Viol, M. Henze, and K. Wehrle, "POSTER : Privacy-preserving Indoor Localization," in *7th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec'14)At: Oxford, United Kingdom*, 2014.

[11] W. Wang, S. Member, Y. Chen, and Q. Zhang, "Privacy-Preserving Location Authentication in Wi-Fi Networks Using Fine-Grained Physical Layer Signatures," vol. 1276, no. c, pp. 1–8, 2015.

[12] S. Kim, S. G. Yoo, and J. Kim, "Privacy Protection Mechanism for Indoor Positioning Systems," *Int. J. Appl. Eng. Res.*, vol. 12, no. 9, pp. 1982–1986, 2017.

[13] I. Agudo, R. Rios, and J. Lopez, "A privacy-aware continuous authentication scheme for proximity-based access control," *Comput. Secur.*, vol. 39, pp. 117–126, 2013.

[14] F. Zhang, A. Kondoro, and S. Muftic, "Location-Based Authentication and Authorization Using Smart Phones," in *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 2012, pp. 1285–1292.

[15] K. Fawaz, K. Kim, and K. G. Shin, "Privacy vs . Reward in Indoor Location-Based Services," 2016, vol. 2016, no. 4, pp. 102–122.

[16] A. Konstantinidis, G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis, "Privacy-Preserving Indoor Localization on Smartphones," *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 11, pp. 3042–3055, 2015.

[17] M. F. Sadikin and M. Kyas, "IMAKA-Tate : secure and efficient privacy preserving for indoor positioning applications," vol. 5760, no. March, 2016.

[18] Z. Yang and K. Järvinen, "The Death and Rebirth of Privacy-Preserving WiFi Fingerprint Localization with Paillier Encryption (Full Version)," in *IEEE International Conference on Computer Communications 2018 (INFOCOM 2018)*, 2018, p. 21.

[19] K. Järvinen *et al.*, "PILOT: Practical Privacy-Preserving Indoor Localization using OuTsourcing," in *4th IEEE European Symposium on Security and Privacy*, 2019, p. 16.

[20] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.