This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

Remote Authentication Schemes for Wireless Body Area Networks Based on the Internet of Things

Mutaz Elradi S. Saeed, Qun-Ying Liu, GuiYun Tian, Bin Gao, Fagen Li
Corresponding authors: Qun-Ying Liu, GuiYun Tian

***Abstract*—Internet of Things is a new technology which offers enormous applications that make people's lives more convenient and enhances cities' development. In particular, smart healthcare applications in IoTs have been receiving increasing attention for industrial and academic research. However, due to the sensitiveness of medical information, security and privacy issues in IoTs healthcare systems are very important. Designing an efficient secure scheme with less computation time and energy consumption is a critical challenge in IoTs healthcare systems. In this paper, a lightweight online/offline certificateless signature (L-OOCLS) is proposed, then a heterogeneous remote anonymous authentication protocol (HRAAP) is designed to enable remote WBANs users to anonymously enjoy healthcare service based on the Internet of Things applications. The proposed L-OOCLS scheme is proven secure in random oracle model and the proposed HRAAP can resist various types of attacks. Compared with the existing relevant schemes, the proposed HRAAP achieves less computation overhead as well as less power consumption on WBANs client. In addition, to nicely meet the application in the IoTs, an application scenario is given.**

***Index Terms*—Public Key Infrastructure, Certificateless Cryptography, Remote Authentication, Anonymity, Wireless Body Area Networks (WBANs), Internet of Things (IoTs).**

I. Introduction

The Internet of Things (IoTs) has been recognised as one of the major technological revolutions of this century [1]. The realisation vision of the IoTs can be achieved with three main architectural components: smart things, back-end servers and communications infrastructure [2]. This vision offers a vast amount of applications such as smart healthcare system, smart grid, intelligent transportation, smart cities, and so on [3]. In particular, smart healthcare applications in IoTs have been receiving increasing attention since they help facilitate remote monitoring of patients. WBANs are formed by various wearable sensors deployed around/in/on the human body [4], where the nodes are connected via wireless communication technologies [5]. WBANs can provide remote monitoring, emergency medical assistance and remote medical treatment with wearable and implantable biosensors [6] [7] [8] [9]. Different types of WBANs sensors collect the vital physiological and environmental information from human body. And then, it transmits the information to remote control center using personal terminal. Finally, the remote control center addresses and analyzes information to meet different requirements [10]. To push the data collected by WBANs into the Internet server, the WBANs need to integrate into the Internet as a part of the IoTs healthcare systems. In fact, the integration has been done and tested according to 6LowPAN standard defined by IETF [11]. Three approaches have been suggested to make this integration: gateway solution, front-end proxy solution and TCP/IP overlay solution [12].

The messages exchanged in the IoTs healthcare systems contain sensitive information about the physical conditions of patients, which is important for patients' privacy. Hence, security and privacy protection is a critical issue, which must be solved in IoTs healthcare systems [13]. In IoTs healthcare systems, information such as the patients' data should only be derived from each patients' devoted WBANs system, and the use of WBANs data should be guaranteed by authorization control strategy. Moreover, the openness and mobility of WBANs lead to more security challenges. For example, an adversary may track a specific patient by linking two or more messages to the same sensor node of the patient, even without identifying the context of this traffic. Besides, an adversary may obtain some critical information about the physical condition of a patient, and these information may help the adversary to launch physical attacks against this patient. In general, IoTs security and privacy challenges especially from technical perspectives such as system limitations, lack of standardization, software vulnerabilities etc. are discussed [14]. In addition, a novel network security model for cooperative virtual networks in the IoTs, which includes network security vulnerabilities, threats, attacks and risks in switches as well as security policy to mitigate those risks is presented [15]. Meanwhile, due to the wearable sensors in WBANs being resource-constrained in terms of memory space, energy supply, computation capabilities and communication rate, security schemes proposed for other networks may not be applicable to IoTs healthcare systems. Thus, in the design of security and privacy schemes for IoTs healthcare systems, the conflicts among efficiency, practicality and security must be considered carefully. The resource-constrained wearable devices in WBANs require the security schemes to be as lightweight and low cost as possible. Security in IoTs healthcare systems should achieve the following requirements [13] [16]: data integrity assurance, data confidentiality, authenticity, non-repudiation, data availability. As is known, based on cryptography, the security mechanisms of IoTs healthcare systems begin from the PKC authentication to ID-PKC authentication, and then to the presently known CL-PKC authentication.

To enhance security, the remote authentication schemes for WBANs have been widely studied to supply anonymous, confidentiality, integrity, non-repudiation and generate session key for encrypting data.

It is worth noting that, as the focus of this paper is on

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

designing a secure scheme to serve security for Healthcare application in IoTs, most of the work in this paper is relevant to the WBANs and IoTs.

TABLE I: The abbreviations and notations used in this paper.

Notation	Description
IoTs	Internet of Things
WBANs	Wireless body area networks
L-OOCLS	Lightweight online/offline cetificateless signature
OOCL-PKS	Online/offline certificateless public key signature
HRAAP	Heterogeneous remote anonymous authentication protocol
TPKC	Traditional public key cryptosystem
PKI	Public key infrastructure
PKC	Public key cryptosystem
ID-PKC	Identity based public key cryptosystem
CL-PKC	Certificateless public key cryptosystem
ECC	Elliptic Curve Cryptography
NM	Network manager
AP	Application provider
KGC	Key generator center
$params$	System parameters
$\mathbb{F}_q$	Finite field with primary order q
1^k	Security parameter
$\mathbb{G}$	The group of elements formed by the points on the elliptic curve $E(\mathbb{F}_q)$ (for ECC-based curve)
$\mathbb{G}_1$	A cycle additive group of order p (for Pairing-based curve)
$\mathbb{G}_2$	A cycle multiplicative group of order p (for Pairing-based curve)
p	A prime order of groups $\mathbb{G}_1$ and $\mathbb{G}_2$
P	A generator of group $\mathbb{G}_1$
$\hat{e}$	A bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$
$H_i()$	A one way hash function, where $i = 1, 2, 3$
s	A master secret key of KGC
P_{pub}	A master public key of KGC
ID_c	An identity of WBANs client
D_c	A partial private key of WBANs client
SK_c	A full private key of WBANs client
PK_c	A public key of WBANs client
s_{NM}	A secret key of network manager
PK_{NM}	A public key of network manager
s_{AP}	A secret key of application provider
PK_{AP}	A public key of application provider
key	A shared key between application provider and WBANs client
$\oplus$	The bitwise XOR operation
$\|$	Concatenation operation
t_c	Current time stamp

II. Related Work

Authentication and/or key agreement for WBANs have been of great interest recently. A few articles that have discussed this issue follow two major mechanisms: non-cryptography and cryptography.

The existing non-cryptography mechanism schemes can be broadly classified into three categories: physiological-signals-based, channel-based and proximity-based. Using the physiological-signals-based, many schemes have been proposed to measure and compare physiological information gathered by the biomedical sensors, such as electrocardiogram (ECG), fingerprint, iris and photoplethysmogram (PPG), to serve authentication and session key establishment without a priori distribution of keying material. The authors in [17] [18] [19] designed their schemes based on physiological-signals-based technique. However, this technique requires different biomedical sensors measuring the same physiological signals of the same person, and that is impossible since it leads to Denial-of-Service attack (DoS). Some schemes based on channel-based technique have been proposed such as [20] [21] [22], where the authors utilized RSS (Received Signal Strength) to assist authentication. However, in fact, the RSS tends to change over time due to the changing environment and nodes mobility. Therefore, it is difficult to obtain a relatively stable RSS profile for a mobile node, what becomes hard to decide if the change of RSS is due to the nodes mobility or an impersonation attack. Moreover, Zeng et al. [20] has not achieved anonymity and Cai et al. [21] required special hardware. In addition, most of the schemes are only applicable in static cases, where the signal, channel, or device characteristics are relatively stable. Given the above issues, their applications are limited. Hence, both schemes are not suitable for practical application in WBANs. The schemes by Kalamandeen et al. [23] and Mathur et al. [24] utilized proximity-based techniques to support authentication and key generation. However, the major drawback of proximity-based technique is that the devices should be within half of the wavelength distance of each other, which constrains the deployment of biomedical sensors in WBANs.

From another perspective, cryptographic mechanisms provide an alternative way of authentication and/ or key generation for WBANs. And most cryptographic schemes have few restrictions of environment and mobility such as channel, distance and location to be applicable. Thus, in the following, we focus on surveying cryptographic mechanisms for authentication and session key establishment related to WBANs.

So far, remote user authentication can be achieved through traditional public key cryptosystem (TPKC) as in [25] [26]. But such schemes are not applicable for WBANs, since TPKC requires to compute modular exponentiation, which may take more computational resource than that the sensor devices can offer. Then, elliptic curve cryptography (ECC) introduced by Miller [27] and Koblitz [28], which offers small key size than TPKC with same security level [29]. For example, 160-bit ECC offers the same security level as 1024-bit RSA. Therefore, ECC is suitable for resource-constrained devices such as sensor. Several schemes based on elliptic curve cryptosystem (ECC) have also been proposed [30] [31] [32] to serve authentication. However, these schemes need PKI (Public Key Infrastructure) to apply ECC, which requires extra computation to verify the certificates of others. Therefore, authentication schemes in [30] [31] [32] are not suitable to apply in WBANs.

It has been seen that the performance of ECC can be enhanced through identity based public key cryptosystem (ID-PKC) [33]. In ID-PKC, the user's secret key is calculated according to his/her identity by a third party called PKG (Private Key Generator) and the identity uses it as the public key of the user. Therefore, the ID-PKC can address the weakness of certificates management inherited by PKI. Various ID-PKC authentication schemes [34] [35] [36] [37] [38] [39] based on ECC have been proposed. Yang et al. [34] proposed remote mutual authentication scheme and they claimed that their scheme was secure. Unfortunately, Yoon et al. [35] pointed out that Yang et al's [34] could not withstand an

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

impersonation attack and does not provide perfect forward secrecy. Subsequently, Islam et al [36] proposed an enhanced remote user mutual authentication scheme to overcome the security weakness of the scheme in [34]. They claimed that their scheme can resist various types of attacks than other existing relevant schemes. However, Truong et al [37] found that the scheme in [36] can not resist denial of service attack. Later, Debiao et al [38] proposed an efficient authentication and key exchange scheme based on ECC, and also claimed that their scheme was secure under random oracle model. Unfortunately, Wang et al [39] pointed out that Debiao et al's [38] is vulnerable to reflection attack and parallel session attack. Lu et al. [40] proposed two SET protocols, SET-IBS and SET-IBOOS for clustered WSN. In SET-IBOOS protocol, an ID-PKC online/offline digital signature is used to reduce the computation overhead. Accordingly, the protocols are tested and analyzed against various attacks. In [41], a novel authentication framework, named ACPN for VANETs is proposed. For the authentication between the RSUs and vehicles, the ACPN framework uses the ID-PKC online/offline signature scheme. Whereas for authentication among vehicles, the ID-PKC signature scheme is used. The ACPN framework is efficient in terms of computation overhead and storage requirement. Recently, the authors in [42] [43] proposed the authenticated secure session key schemes based on ID-PKC. However, the scheme in [42] has not achieved the anonymity property. Nonetheless, all the above schemes are not suitable for WBANs applications since some schemes being vulnerable to some attacks and/or not having a user anonymity presented. Besides, some schemes are designed for mobile devices, which offer more resources than that sensor devices can offer. Moreover, the ID-PKC suffers from key escrow problem since the PKG knows all private keys of clients.

Al-Riyami and Paterson introduced the certificateless public key cryptography CL-PKC [44] to overcome the key escrow weakness inherited by ID-PKC and certificate management problem inherited by PKI. In the CL-PKC, the full private key of user comprised of two parts: one comes from third trust party called KGC (Key Generation Center) and the other is created by the user. As a result, the CL-PKC is the best choice for resource-constrained devices such as sensor node. Recently, some remote anonymity authentication and session key establishment schemes for WBANs have been proposed [45] [46] [47] [48] [49]. Liu et al [45] utilized CL-PKC to design lightweight signature scheme, in which the authentication protocol with session key establishment is derived by using their signature scheme. However, Xiong [46] demonstrated that the scheme in [45] cannot resist public key replacement attack when the adversary makes query for public key replacement, and it is lack of forward secrecy. And then he proposed a secure remote anonymity authentication scheme using CL-PKC. Moreover, the computation overhead is reduced. Consequently, Zhao [47] utilized ECC to propose an efficient anonymous authentication scheme. Unfortunately, Wang and Zhang [48] pointed out that Zhao's [47] scheme has not achieved the unlinkability of a user. And then, they proposed a new anonymous authentication scheme to overcome the weakness of the previous scheme. He et al. [49] found that the scheme proposed by Liu et al [45] was vulnerable to an impersonation attack, and then they proposed a remote anonymous authentication scheme. Their scheme did really resist various forms of attacks. In addition, the schemes in [47] [48] were designed based on ID-PKC, which have a key escrow problem. Moreover, the schemes in [46] [49] have more computation overhead. Furthermore, CL-PKC does not scale well at the Internet side. The authors in [50] [51] proposed a multi-layer authentication protocol and a secure session key establishment method for WBANs. However, their protocols do not achieve the end-to-end security since each one has two session keys; the one key is used to encrypt data between sensor node and local server, the other key is used to encrypt data between local server and AP. In addition, the group key between sensor nodes and local server in [50] requires to be updated in case of node deletion or addition.

It is observed that the above reviewed authentication and session key establishment schemes suffer from either, some schemes being vulnerable to some attacks separately and/or having more computation overhead, which results in more energy consumption than other schemes that have low computation overhead. Besides, some schemes do not achieve end-to-end security or are not scalable well at the Internet side since the CL-PKC is used.

The concept of online/offline technique was introduced by Even et al. [52]. Their scheme has presented a methodology to transform any signature into two phases: online phase and offline phase. In the offline phase, most of the heavy operations are done before a message is known. In the online phase, only lightweight operations are done by using a precomputation of the offline phase and the message to produce a signature. This technique can help the researchers to design lightweight secure schemes to be applicable for resource-constrained devices.

A. Contributions and Organization

To address the above issues presented in the related work Section, a heterogeneous remote anonymous authentication protocol (HRAAP) is proposed. The HRAAP can be used for authentication and session key establishment between WBANs client and AP (Application Provider) based on the applications of Internet of Things. The contributions of this work are as follows:

- In this paper, a lightweight online/offline certificateless signature scheme is proposed, which is provably secure against existential forgery adaptively chosen message attacks in the random oracle model [58]. Then, a heterogeneous remote anonymity authentication protocol (HRAAP) to serve authentication and session key establishment for WBANs in the IoTs application is derived.
- To reduce the computation overhead in WBANs client, an online/offline technique is used. Moreover, to overcome the key escrow problem inherited by ID-PKC (Identity based Public Key Cryptosystem), the CL-PKC (Certificateless Public Key Cryptosystem) is used. Furthermore, to be more scalable in AP, the PKC (Public Key Cryptosystem) is used.

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

- To show the performance of the proposed HRAAP in terms of computation overhead and energy consumption, the comparison between the HRAAP and relevant existing work are studied. The results show that, the proposed HRAAP is most efficient in terms of computation overhead as well as energy consumption.
- In order to show the feasibility of HRAAP on resisting attacks, the security analysis is given. The results show that the proposed HRAAP can resist various types of attacks. Furthermore, to nicely meet the application in the IoTs, an application scenario is given.

Consequently, the proposed schemes can be applied to serve security on WBANs in IoTs applications which comprise of resource-constrained devices. They can also be applicable to powerful devices resulting in serving security for other applications.

The remaining sections of this paper are organized as follows: Section III gives a brief introduction to bilinear pairings and security assumptions related to the proposed schemes. Section IV provides the framework of OOCLS scheme. Section V presents the network architecture of HRAAP as well as security threats. The proposed L-OOCLS scheme and its security analysis in random oracle model are given in Section VI. Section VII presents the proposed HRAAP. The security analysis and quantitative performance of HRAAP are given in Section VIII. An application scenario is described in Section IX. Conclusion and future work are drawn in last Section.

III. Preliminaries

This section presents the properties of bilinear pairings and basic definitions of intractable assumptions, on which the proposed schemes rely.

A. Notation

In order to clearly understand the proposed schemes, the abbreviations and notations used are listed and their meanings are given in Table I.

B. Bilinear Pairings

Let $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, *)$ be two cyclic groups, $\mathbb{G}_1$ is an additive group of elliptic curve generated by P with prime order p and $\mathbb{G}_2$ is a multiplicative group of finite field with the same prime order of $\mathbb{G}_1$. The bilinear pairing is defined as a map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. It is assumed that elliptic curve discrete logarithm problem (ECDLP) is intractable in $\mathbb{G}_1$ and discrete logarithm problem is intractable in $\mathbb{G}_2$. A bilinear pairing satisfies the following properties:

1) Bilinearity: $\forall P, Q \in \mathbb{G}_1$, and $\forall a, b \in \mathbb{Z}_p^*$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
2) Non-degeneracy: there exists $P, Q \in \mathbb{G}_1$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_2}$, where $1_{\mathbb{G}_2}$ represents the identity of group $\mathbb{G}_2$.
3) Computability: $\forall P, Q \in \mathbb{G}_1$, there exists an efficient algorithm to compute $\hat{e}(P, Q)$.

Formally, a symmetric pairing defined over elliptic curve can be computed by the Tate pairing [57] or by the η_T pairing [60]. An efficient algorithm takes as input a security parameter 1^k, and returns specification of groups $\mathbb{G}_1$, $\mathbb{G}_2$ and a bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

C. Intractability Problems

Let $\mathbb{G}_1$ be an additive cyclic group of prime order p and generator P. To ensure the security of proposed schemes, the following intractability assumptions are used in $\mathbb{G}_1$:

Definition 1: let $\mathbb{G}_1$ be cyclic group of prime order p and P be a generator of $\mathbb{G}_1$, the q-strong Diffie-Hellman Problem (q-SDHP) in $\mathbb{G}_1$ is given a$(q+1)$-tuple $(P, \alpha P, \alpha^2 P, ..., \alpha^q P) \in \mathbb{G}_1$ as input. It is difficult to find a pair $(\lambda, \frac{1}{\lambda+\alpha} P)$, where $\lambda, \alpha \in \mathbb{Z}_p^*$ [71].

Definition 2: let $\mathbb{G}_1$ be cyclic group of prime order p and P be a generator of $\mathbb{G}_1$, the Elliptic Curve Discrete Logarithm Problem (ECDLP) in $\mathbb{G}_1$ is given a tuple $(P, xP) \in \mathbb{G}_1$ as input. It is impossible to extract $x \in \mathbb{Z}_p^*$ [59].

Definition 3: let $\mathbb{G}_1$ be cyclic group of prime order p and P be a generator of $\mathbb{G}_1$, the Computational Diffie-Hellman Problem (CDHP) in $\mathbb{G}_1$ is given a tuple $(P, aP, bP) \in \mathbb{G}_1$ as input. It is difficult to compute $abP \in \mathbb{G}_1$, where $a, b \in \mathbb{Z}_p^*$.

Definition 4: let $\mathbb{G}_1$ be cyclic group of prime order p and P be a generator of $\mathbb{G}_1$, the Inverse Computational Diffie-Hellman Problem (Inv-CDHP) in $\mathbb{G}_1$ is given a tuple $(P, xP) \in \mathbb{G}_1$ as input. It is hard to compute $x^{-1}P \in \mathbb{G}_1$, where $x \in \mathbb{Z}_p^*$.

IV. Framework of OOCLS Scheme

OOCLS is an online/offline certificateless signature scheme, which allows the WBANs client (sensor node) in CL-PKC (Certificateless Public-Key Cryptosystem) domain to send a signed message to the AP in the PKC (Public Key Cryptosystem) domain. Moreover, to minimize the computational overhead in CL-PKC domain, online/offline techniques are used [52]. An OOCLS framework which includes generic model and security model of OOCLS scheme is described as follows:

A. Generic Model

According to the definitions in [44] [67] [68] for ordinary certificateless signature schemes, the formal structure of OOCLS scheme consists of the following algorithms:

- Setup(1^k): the global setup algorithm, which takes a security parameter 1^k as input, and returns KGC's secret key s and $params$ (system parameters) including a master public key P_{pub}, gives $params$ to all clients in WBANs and AP. This algorithm is executed by KGC for an initial setup of the system.
- Set Public-Key($ID_c, params$): an algorithm is run by the WBANs client, in which client's identity ID_c and $params$ are taken as input, then client's public key

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

$PK_c \in \mathbb{G}_1$ and secret value $x_c \in \mathbb{Z}_p^*$ are outputted. The resulting public key is assumed to be publicly known.

- Extract Partial-Private-Key($PK_c, s, params$): a deterministic algorithm is run by the KGC, in which client's public key PK_c, KGC's secret key s and $params$ are taken as input, then a partial private key of client D_c is returned.
- Set Full-Private-Key(D_c, x_c,): an algorithm is run by the WBANs client, in which client's partial private key D_c and secret value x_c that is generated with client's public key are taken as input, then a full private key SK_c is outputted.
- CL-OffSign($PK_c, SK_c, x_c, P_{pub}, params$): the certificateless offline signature algorithm is run by inputting the client's public key PK_c, full private key SK_c and secret value x_c. It also has the PKG's public key P_{pub} and $params$ as input, then it returns CL-OffSig result $\sigma_c^{'}$ ($\sigma_c^{'} = \gamma, y, \Gamma, Q_c, W_c$, where $y, \gamma \in \mathbb{Z}_p^*$). It should be noted that, this algorithm is run by a powerful trustworthy device and works without knowledge of a message.
- CL-OnSign($\sigma_c^{'}, params, m$): the probabilistic certificateless online signature algorithm is run by inputing a CL-OffSign $\sigma_c^{'}$, a message $m \in \mathcal{M}$ and $params$, then a full signature σ_c is generated. Where $\mathcal{M}$ is a message space.
- Verification($\sigma_c, Q_c, W_c, params, m$): the deterministic verification algorithm is run by inputing a signature σ_c, Q_c, W_c, $params$ and message m. This algorithm outputs 1, which means that the signature is valid on a message m. If it outputs 0, it means that the signature is invalid.

It should be noted that, the above algorithms must satisfy the standard consistency constrain of OOCLS as follows.

for all $k \in \mathbb{N}$, $ID_c \in \{0,1\}^*$ and $m \in \mathcal{M}$
If $\sigma_c^{'}$ = CL-OffSign($PK_c, SK_c, x_c, P_{pub}, params$) and
σ_c = CL-OnSign($\sigma_c^{'}, params, m$), then
1 = Verification($\sigma_c, Q_c, W_c, params, m$)

B. Security Model of OOCLS Scheme

This subsection demonstrates the security model of OOCLS scheme. As is defined in [44] [67] [68], the security of a certificateless signature scheme can be analyzed by considering two types of adversaries, Type I adversary $\mathcal{A}_I$ and Type II adversary $\mathcal{A}_{II}$, since the sender belongs to the CL-PKC domain [44]. Type I Adversary $\mathcal{A}_I$ represents a third party attacker against the OOCLS scheme. That is, adversary $\mathcal{A}_I$ does not allow access to the master secret key s, but has the ability to replace the public keys of any entity with a value of its choice. Type II Adversary $\mathcal{A}_{II}$ represents a malicious KGC. Here, the adversary $\mathcal{A}_{II}$ is equipped with the KGC's secret key s, but cannot replace any client's public key. In fact, if the adversary $\mathcal{A}_{II}$ is allowed to replace a client's public key, then the adversary can easily forge the signature of the client. Whereas, the sender in the OOCLS scheme belongs to the certificateless public key. Hence, the scheme should achieve unforgeability (unforgeability against adaptive chosen messages attacks: UF-CMA). The security notions in [67] [69] [70] are modified to adapt the OOCLS scheme. The games for security notions are described as follows.

Existential Unforgeability Games: here two types of adversaries, Type I adversary $\mathcal{A}_I$ and Type II adversary $\mathcal{A}_{II}$ (EUF-CMA-I game and EUF-CMA-II game) are considered.

EUF-CMA-I Game: in this game, the challenger $\mathcal{C}$ interacts with Type I adversary $\mathcal{A}_I$ as follows.

Initialization Phase: the challenger $\mathcal{C}$ runs the setup algorithm on the input of a security parameter 1^k for generating master secret key s and public $params$. $\mathcal{C}$ keeps s and then gives $params$ to $\mathcal{A}_I$. It should be noted that, $\mathcal{A}_I$ does not know the s.

Attack Phase: an adversary $\mathcal{A}_I$ can perform a polynomial bounded number of oracle queries in an adaptive way as follows:

- Request Public-Key: upon receiving a public key query for any identity ID_c, C runs public key generation algorithm and returns PK_c to $\mathcal{A}_I$. Then, it keeps a list for its queries. The secret value x_c output of this query is one which is used to generate ID's public key PK_c.
- Request Partial-Private-Key: an adversary $\mathcal{A}_I$ is able to perform query for the partial private key D_c for any identity ID_c except the challenged identity ID_c^*. The challenger $\mathcal{C}$ computes the partial private key D_c and returns it to $\mathcal{A}_I$.
- Request Full-Private-Key: an adversary $\mathcal{A}_I$ is able to ask full private key SK_c query for any ID_c except the challenged identity ID_c^*. $\mathcal{C}$ computes the full private key SK_c corresponding to the identity ID_c and returns it to $\mathcal{A}_I$.
- Replace Public-Key: for any identity ID_c, an adversary $\mathcal{A}_I$ can pick a new secret value $x_c^{'}$ and compute the new public key $PK_c^{'}$ in the public key space $\mathcal{PK}$, and then replace PK_c with $PK_c^{'}$. It should be noted that, It is not required for $\mathcal{A}_I$ to provide the corresponding secret value $x_c^{'}$ when making this query.
- Signing Oracle Queries: an adversary $\mathcal{A}_I$ may need to ask a signing query. It submits a message m and a sender's identity ID_c. The challenger $\mathcal{C}$ finds sender's private key SK_c and public key PK_c (C may need to run corresponding algorithms to generate those keys). $\mathcal{C}$ runs the CL-OffSign($PK_c, SK_c, x_c, P_{pub}, params$) to obtain $\sigma_c^{'}$. Finally, $\mathcal{C}$ runs the CL-OnSign($\sigma_c^{'}, params, m$) algorithm to obtain σ_c. Then, it sends σ_c, Q_c, W_c and m to $\mathcal{A}_I$. If the public key PK_c has been replaced by $\mathcal{A}_I$. In such a case, an adversary $\mathcal{A}_I$ needs to submit the secret value $x_c^{'}$ corresponding to the replaced public key $PK_c^{'}$ to the signing oracle.
- Output Phase: after all queries, $\mathcal{A}_I$ outputs a forgery($\sigma_c^*, Q_c^*, W_c^*, ID_c^*, m^*$), where ID_c^* is the challenged identity. Finally, $\mathcal{A}_I$ wins the game if the following conditions hold:
  - Request Full-Private-Key (ID_c^*) has never been queried
  - Request Partial-Private-Key (ID_c^*) and Replace Public-Key($ID_c^*, PK_c^{*'}$) have never been queried

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

- $\mathcal{A}_I$ has never submitted m^* to the signing oracle with respect to the challenged identity ID_c^*
- $1 \longleftarrow \text{Verify}(\sigma_c^*, Q_c^*, W_c^*, params, m^*)$

Definition 5: an OOCLS scheme is EUF-CMA-I secure if the advantages of probabilistic polynomial time adversary $\mathcal{A}_I$ is negligible ϵ after at most perform attack phase queries in the UF-CMA-I game.

EUF-CMA-II Game: this is a game in which challenger $\mathcal{C}$ interacts with Type II adversary $\mathcal{A}_{II}$ as follows.

Initialization Phase: the challenger $\mathcal{C}$ runs the setup algorithm to generate a master key s and $params$. $\mathcal{C}$ gives both KGC's secret key s and $params$ to $\mathcal{A}_{II}$.

Attack Phase: an adversary $\mathcal{A}_{II}$ may perform a polynomial bounded number of oracle queries: Request Public-Key, Request Full-Private-Key and Signing Oracle queries in an adaptive way as defined in EUF-CMA-I Game. It should be noted that, here the adversary $\mathcal{A}_{II}$ can compute the Partial-Private-Key D_c of an identity ID_c since it knows the master secret key s.

- Output Phase: after all queries, A_{II} produces a forgery$(\sigma_c^*, Q_c^*, W_c^*, ID_c^*, m^*)$, where ID_c^* is challenged identity. Finally, $\mathcal{A}_{II}$ wins the game if the following conditions hold:
  - Request Full-Private-Key(ID_c^*) query has never been queried
  - Signing Oracle on m^* and ID_c^* with respect challenged identity ID_c^* has never been quired
  - $1 \longleftarrow \text{Verify}(\sigma_c^*, Q_c^*, W_c^*, params, m^*)$

Definition 6: an OOCLS scheme is EUF-CMA-II secure if the advantages of probabilistic polynomial time adversary $\mathcal{A}_{II}$ is negligible ϵ after the most attack phase queries in the UF-CMA-II game is performed.

Definition 7: an OOCLS scheme is said to be existentially unforgeable against adaptive chosen message attacks (EUF-CMA), if the success probability of both $\mathcal{A}_I$ and $\mathcal{A}_{II}$ is negligible.

V. System Description and Objective of HRAAP

In this section, the network architecture of proposed HRAAP and its components, and the potential threats of establishing a shared key as well as protocol's objectives are presented.

A. Network Architecture and Components

As is shown in Fig. 1, the HRAAP comprises of three main parts: Network Manager (NM), WBANs clients and AP (Application Provider). The system model is described as follows:

- Network Manager (NM): it is in charge of an enrolling system setup, and registration of WBANs clients and APs. It is semi-trusted, since it has the knowledge of partial private keys of WBANs clients (The WBANs clients belong to the certificateless public key cryptosystem) and public parameters of AP (AP belong to the public key cryptosystem). Therefore, the NM cannot impersonate the WBANs clients or AP without being detected, resulting in overcoming the key escrow problem inherited by ID-PKC.
- WBANs clients: WBANs contain sensor nodes as WBANs clients that gather data from patients, and then send them to the AP via an Internet medium. Before sending data to the AP, each WBANs client should be registered with NM and preloaded with partial private key and public parameters. In addition, the WBANs client computes its full private key, and creates a shared key AP. This key is used for future communication between WBANs client and AP.
- Application Provider (AP): it works as database server, which is in charge of storing the data coming from WBANs clients and provides them to the physicians through web interface. The AP needs to receive system parameters from NM, as well as sends its public key to NM. Finally, it needs to generate a shared key with each WBANs client. The shared key is used for secure communication between them.

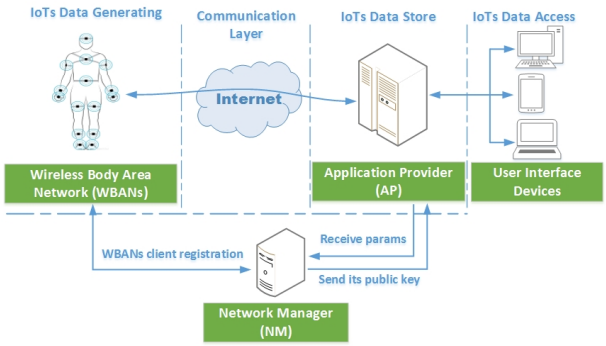

Fig. 1: Network architecture and components of HRAAP based on IoTs

B. Security Threats of HRAAP

Through key establishing between WBANs client and AP, the HRAAP is vulnerable to a number of security attacks. In the following, some of these attacks are presented:

- Anonymity Attack: the goal of this attack is to try to reveal the identity of the patient when WBANs and AP exchange the messages on session key establishment process. To achieve the anonymity property, the identity of a patient should remain unknown to an eavesdropper. Countermeasures to these attacks are data encryption, which hides the contents of messages.
- Linkability Attack: here the attacker can directly link two particular messages as being part of different sessions performed by the same WBANs client or AP. Therefore, if the attacker learns anything about WBANs client/AP repeating sessions, unlinkability will fail. It should be noted that unlinkability does not imply anonymity property. Countermeasures to these attacks are data encryption, which hides the contents of messages.
- Repudiation Attack: repudiation refers to a denial of legal entity in all or part of communications in IoTs healthcare

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

systems. For instance, an AP could deny WBANs client to create a share key or vice versa. Therefore, non-repudiation refers to the ability of a system to assure that something that is actually valid cannot be denied or counters repudiation threats. Countermeasures to these attacks are data authentication, where the receiver authenticates the sender of a message.

- Replay Attack: it is a category of network attack. Its goal is to replay a message that is originally sent by a legitimate WBANs client/AP to make the entity that receives the message be busy or unavailable. A countermeasure to avoid a message replay attack is to ensure the freshness of message, for instance, via attaching a time stamp with each message.
- Impersonation Attack: an adversary attempts to impersonate the target user (WBANs client or AP) without knowing the target user's secret. Countermeasures to these attacks are data authentication, where the receiver authenticates the sender of a message.

The goal of the proposed HRAAP is to generate anonymous authenticated key between WBANs client and AP. The shared key can be used to build a secure channel for data transmissions between them. Meanwhile, as is seen in the related work, the existing relevant anonymous authenticated keys for WBANs suffer from either, some schemes being vulnerable to some attacks separately and/or having more computation overhead that leads to more energy consumption, which is a critical issue in a resource-constrained device. Besides, some schemes are designed based on the ID-PKC, which has key escrow problem or are not well scalable at the Internet side.

In this work, we aim to propose the anonymous authenticated session key establishment that can resist various security threats. Moreover, it can achieve efficient computation overhead as well as energy consumption. Furthermore, it should be better scalable at the Internet side.

VI. Lightweight Online/Offline Certificateless Signature Scheme (L-OOCLS)

In this section the proposed L-OOCLS signature and its security analysis in random oracle model are given.

A. The L-OOCLS Scheme

The proposed L-OOCLS scheme consists of five algorithms: System Setup (Setup), WBANs Client Key Generation, Certificateless Offline Signature (CL-OffSign), Certificateless Online Signature (CL-OnSign) and Verification.

Setup: input a security parameter 1^k, the KGC chooses two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p ($\mathbb{G}_1$ additive group and $\mathbb{G}_2$ multiplicative group), a generator P of $\mathbb{G}_1$ and a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Moreover, there are three hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_2 : \mathbb{G}_1 \rightarrow \mathbb{Z}_p^*$, $H_3 : \{0,1\}^n \times \mathbb{G}_2 \rightarrow \mathbb{Z}_p^*$, where n is the number of message bits. The KGC selects randomly $s \in \mathbb{Z}_p^*$ as master secret key, then computes its master public key $P_{pub} = sP$. The KGC publishes the system parameters $(\mathbb{G}_1, \mathbb{G}_2, \hat{e}, p, P, P_{pub}, g, H_1, H_2, H_3)$ and keeps the master secret key s as private, where $g = \hat{e}(P, P)$.

WBANs Client Key Generation: in the proposed L-OOCLS scheme, all WBANs clients (sensor nodes) belong to the CL-PKC domain. The WBANs client keys are computed as follows:

- Public Key of WBANs client (ID_c): the client with identity ID_c chooses a secret value $x_c \in \mathbb{Z}_p^*$ randomly, then computes its public key as follows:

$$PK_c = x_c H_1(ID_c)P$$

- Partial Private Key of WBANs client (PK_c): the client with identity ID_c transmits its public key PK_c to the KGC. The KGC calculates the partial private key of client as follows:

$$D_c = (H_2(PK_c) + s)^{-1}P$$

Then D_c is sent to the WBANs client in a secure channel.

- Full Private Key of WBANs client (D_c, x_c): this algorithm takes as input a secret value x_c and partial private key D_c of client with identity ID_c. Then the full private key of client is computed as follows:

$$SK_c = (x_c)^{-1}D_c$$

The message m is signed by WBANs client and is verified by AP as follows:

CL-OffSign $(SK_c, PK_c, x_c, P_{pub}, params)$: the algorithm takes as input full private key SK_c and public key PK_c of client with identity ID_c, a secret value x_c, KGC's public key P_{pub} and $params$, then computes offline signature $\sigma_c^{'}$. This algorithm works as follows:

1) Pick $\gamma, y \in \mathbb{Z}_p^*$ randomly
2) Compute $\Gamma = g^y$
3) Compute $Q_c = x_c H_2(PK_c)P$
4) Compute $W_c = x_c P_{pub}$
5) Compute $\mu_c = \gamma^{-1} SK_c$
6) Output offline signature $\sigma_c^{'} = (\gamma, y, \Gamma, \mu_c, Q_c, W_c)$

It should be noted that, the computation of this algorithm is performed by a powerful device and the result is stored in the WBANs client before deployment. In addition, the powerful device should be trustful.

CL-OnSign $(\sigma_c^{'}, params, m)$: the algorithm takes an offsign result $\sigma_c^{'}$, $params$ and message m as input, then computes the signature as follows:

1) Compute $h_c = H_3(m, \Gamma) \in \mathbb{Z}_p^*$.
2) Compute $\beta_c = (y + h_c)\gamma \ mod \ p$.
3) Output the signature $\sigma_c = (h_c, \beta_c, \mu_c) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^* \times \mathbb{G}_1$ on the message $m \in \mathcal{M}$, where $\mathcal{M}$ is a messages space.
4) The WBANs client sends σ_c, Q_c, W_c and m to AP.

Verification $(\sigma_c, Q_c, W_c, params, m)$: the algorithm takes a signature σ_c, Q_c, W_c, $params$ and a message m, then check the validity. This algorithm works as follows:

1) Compute $S_c = \beta_c \mu_c$
2) Check whether $h_c \stackrel{?}{=} H_3(m, \hat{e}(S_c, Q_c + W_c)g^{-h_c})$. If it is, accept the message m. Otherwise, reject the message.

Consistency: The consistency of verification is as follows:

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

$$
\begin{aligned}
h_c &= H_3(m, \hat{e}(S_c, Q_c + W_c)g^{-h_c}) \\
&= H_3(m, \hat{e}((y + h_c)SK_c, x_c H_2(PK_c)P + x_c P_{pub})g^{-h_c}) \\
&= H_3(m, \hat{e}((y + h_c)\tfrac{D_c}{x_c}, x_c(H_2(PK_c) + s)P)g^{-h_c}) \\
&= H_3(m, \hat{e}((y + h_c)\tfrac{1}{x_c}\tfrac{1}{H_2(PK_c)+s}P, \\
&\quad x_c(H_2(PK_c) + s)P)g^{-h_c}) \\
&= H_3(m, \hat{e}((y + h_c)P, P)g^{-h_c}) \\
&= H_3(m, \hat{e}(P, P)^{(y+h_c)}g^{-h_c}) \\
&= H_3(m, g^{(y+h_c)}g^{-h_c}) \\
&= H_3(m, g^y) \\
&= H_3(m, \Gamma) \\
&= h_c
\end{aligned}
$$

In Fig. 2, the phases of proposed L-OOCLS scheme is described.

B. Security Analysis of L-OOCLS Scheme

This subsection demonstrates that, the proposed L-OOCLS scheme is proved to be secure in EUF-CMA property.

Theorem 1: the proposed L-OOCLS scheme is EUF-CMA secure in the random oracle model under the assumptions that q-SDH and Inv-CDHP in $\mathbb{G}_1$ are intractable.

Proof: the Theorem 1 using Lemmas 1 and 2 is proved as follows.

Lemma 1 (Unforgeability, Type I adversary $\mathcal{A}_I$): if there exists a probabilistic polynomial-time (ϵ, t, q)-adversary $\mathcal{A}_1$, which has an advantage $\epsilon \geq 10(q_{Sig}+1)(q_{Sig}+q_{H_3})/2^k$ against the EUF-CMA-I security of L-OOCLS scheme, after running in a time t and making q_{H_i} queries to random oracles $H_i(i = 1, 2)$, q_{pk} queries to public-key, q_{ppk} partial-private-key queries, q_{sk} queries to private-key, q_{pkr} public-key replacement queries and q_{sig} signing oracle queries. Then, there exists a $(t^{'})$-algorithm $\mathcal{C}$ that can solve the q-SDH problem in $\mathbb{G}_1$ for $q = q_{H_1}$ in an expected time

$t^{'} \leq 120686 q_{H_3} \frac{(t+O(q_{sig}t_p))}{\epsilon(1-1/2^k)(1-q/2^k)} + O(q^2 t_{sm})$,

where notations t_p and t_{sm} respectively denotes the running time of computing a pairing operation in $\mathbb{G}_2$ and the required time for a scalar multiplication in $\mathbb{G}_1$.

Proof. See appendix A

Lemma II (Unforgeability, Type II adversary $\mathcal{A}_{II}$): if there exists a probabilistic polynomial-time (ϵ, t, q)-adversary $\mathcal{A}_{II}$, which has an advantage $\epsilon \geq 10(q_{Sig}+1)(q_{Sig}+q_{H_3})/2^k$ against the EUF-CMA-II security of L-OOCLS scheme, after running in a time t and making q_{H_i} queries to random oracles $H_i(i = 1, 2)$, q_{pk} queries to public-key, q_{sk} queries to private-key and q_{sig} signing oracle queries. Then, there exists a $(t^{'})$-algorithm $\mathcal{C}$ that is able to solve the Inv-CDHP problem in $\mathbb{G}_1$ for $q = q_{H_1}$ in an expected time

$t^{'} \leq 120686 q_{H_3} \frac{(t+O(q_{sig}t_p))}{\epsilon(1-1/2^k)} + O(q^2 t_{sm})$,

where t_p denotes the running time of computing a pairing operation in $\mathbb{G}_2$ and t_{sm} denotes the required time for one scalar multiplication in $\mathbb{G}_1$.

Proof. See appendix B

VII. Heterogeneous Remote Anonymous Authentication Protocol (HRAAP)

To meet the lightweight security demands of WBANs, the new L-OOCLS scheme is used to design heterogeneous remote authentication protocol, which can preserve the remote anonymous authentication with session key establishment between WBANs client and AP, and save computation overhead as well as energy consumption. In the following, how to design the architecture and preliminary vision of HRAAP are presented.

A. Design Architecture

As is shown in Fig. 1, the HRAAP protocol comprises of three main parts: NM (Network Manager), WBANs clients and AP (Application Provider). In particular, WBANs contain biosensors as clients that gather data from patients, then sends them to the AP via Internet medium. APs work as database server, which are in charge of storing patients' data and provide those data to the users such as physicians. In addition, there is a semi-trustworthy third party named NM which serves as a key generator for WBANs clients. Also, it generates system parameters $params$.

B. Preliminary Vision HRAAP

In principle, the proposed heterogeneous remote anonymous authentication protocol takes the new L-OOCLS scheme proposed in Section VI. as the design basis. NM first generates its private/public key, system parameters $params$ and WBANs clients' partial private keys. In addition, AP generates its private/public key, and then sends its public key to NM. To log in, a WBANs client needs to send a ciphertext, a special parameter and time stamp to the corresponding AP, who then extracts the client's signature and a message m, and validates the signature. Finally, the AP computes a key of the current session and sends MAC (Message Authentication Code) with a special parameter to WBANs client as response of service request. The proposed HRAAP consists of three algorithms: Initialization, Registration and Authentication. These algorithms can be formally shown as follows:

1) Initialization: the NM works as KGC, it generates keys and creates an enrollment system. In this step, given security parameter 1^k, NM generates its private/public key pair $\langle s_{NM}, PK_{NM}\rangle$, where $s_{NM} \in \mathbb{Z}_p^*$ and $PK_{NM} = s_{NM}P$. Then, it publicizes the $params$ $\langle \mathbb{G}_1, \mathbb{G}_2, p, P, g, \hat{e}, PK_{NM}, H_1, H_2, H_3, H_4, H_5\rangle$ as described in Section VI., where $H_4 : \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_p^*$ and $H_5 : \mathbb{G}_1 \rightarrow \mathbb{Z}_p^{*^3} \times \mathbb{G}_1^3 \times \{0,1\}^*$. Moreover, it is supposed that each AP also has a long-term private/public key $\langle s_{AP}, PK_{AP}\rangle$, where $s_{AP} \in \mathbb{Z}_p^*$ and $PK_{AP} = s_{AP}P$.

2) Registration: WBANs client with identity ID_c should perform the following operation with NM to access an AP of interest:
   a) A legitimate WBANs client generates its public key PK_c and sends it to NM as described in Section VI.

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

Fig. 2: Remote Authentication Schemes

WBANs Client	Public channel	Application Provider (AP)
L-OOCLS Phases: CL-OffSign - $\gamma, y \in \mathbb{Z}_p^*$ randomly - $\Gamma = g^y$ - $Q_c = x_c H_2(PK_c)P$ - $W_c = x_c P_{pub}$ - $\mu_c = \gamma^{-1} SK_c$ - Output offsign $\sigma_c^{'} = (\gamma, y, \mu_c, \Gamma, Q_c, W_c)$ CL-OnSign - $h_c = H_3(m, \Gamma) \in \mathbb{Z}_p^*$ - $\beta_c = (y + h_c)\gamma \ mod \ p$ - Output signature $\sigma_c = (h_c, \beta_c, \mu_c)$ - Send σ_c, Q_c, W_c and m	$\xrightarrow{\langle \sigma_c, Q_c, W_c, m \rangle}$	Verification $S_c = \beta_c \mu_c$ $h_c \stackrel{?}{=} H_3(m, \hat{e}(S_c, Q_c + W_c) g^{-h_c})$
HRAAP Phases: - $ind_c = H_4(right, PK_c)$ - Let $m = right \| ind_c$ - Sign a message m using L-OOCLS to get σ_c, Q_c and W_c - $\alpha \in \mathbb{Z}_p^*$ randomly - $\theta = \alpha P$ - $\theta^{'} = \alpha P K_{AP}$ - $\theta_h = H_5(\theta)$ - $C = (\sigma_c \| Q_c \| W_c \| m) \oplus \theta_h$ - Pick current time stamp t_c, then compute $h_c = H_4(\sigma_c \| t_c, \theta)$ - Send $Req = (C, t_c, \theta^{'})$	$\xrightarrow{\langle Req = C, t_c, \theta^{'} \rangle}$	- Check the freshness of t_c - $\theta = s_{AP}^{-1} \theta^{'}$ - $\theta_h = H_5(\theta)$ - Extract $\sigma_c \| Q_c \| W_c \| m = C \oplus \theta_h$ - Verify $\langle \sigma_c, m \rangle$ and check validity of $h_c \stackrel{?}{=} H_4(\sigma_c \| t_c, \theta)$ hold or not - Extract $right \parallel ind_c = m$ - Search client by indexed ind_c - $\tau \in \mathbb{Z}_P^*$ randomly - $K = \tau\theta$ and $\psi = \tau P$ - The session key $key = H_4(h_c, K)$ - Compute $MAC_{key}(h_c)$ - Send $MAC_{key}(h_c)$ and ψ as the reply
	$\xleftarrow{\langle Reply = MAC_{key}(h_c), \psi \rangle}$	
- $K = \alpha\psi$ - The session key $key = H_4(h_c, K)$ - Checks the integrity of $MAC_{key}(h_c)$ with session key key		

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

b) Upon receiving public key PK_c of WBANs client, NM computes his/her partial private key D_c as described in Section VI., and defines his/her $right$, where $right$ indicates to assist information such as service type. Then, it issues $\{D_c, right\}$ to WBANs client. It should be noted that, NM delivers $\{D_c, right\}$ to WBANs client in a secure channel. In addition, NM creates an account for WBANs client in the form of $\langle ind_c \rangle$, where $ind_c = H_4(right, PK_c)$. Then it sends ind_c to AP via a secure channel such as SSL (Secure Socket Layer).
c) Upon receiving $\{D_c, right\}$, WBANs client computes its full private key SK_c as described in Section VI., then stores $\{right, SK_c\}$ securely.
d) AP sends its public key PK_{AP} to NM for registration, then it receives the system parameters.

In the same way, WBANs client can store a group of PK_{AP} for different APs of interest. Moreover, system $params$ and MAC (Message Authentication Code) denoted as $MAC_{(.)}(.)$, are loaded simultaneously for login phase.

3) Authentication: The WBANs client needs to perform the following operations to authenticate himself to the AP of interest:
a) Compute $ind_c = H_4(right, PK_c)$
b) Let $m = right \| ind_c$
c) Sign a message m using L-OOCLS to get σ_c, Q_c and W_c
d) Choose $\alpha \in \mathbb{Z}_p^*$ randomly, then compute $\theta = \alpha P$, and compute $\theta^{'} = \alpha PK_{AP}$.
e) Compute $\theta_h = H_5(\theta)$
f) Compute $C = (\sigma_c \| Q_c \| W_c \| m) \oplus \theta_h$
g) Pick up the current time t_c, then compute $h_c = H_4(\sigma_c \| t_c, \theta)$, where σ_c is the signature of m
h) Send a service request message $Req = (C, t_c, \theta^{'})$.

When the AP receives $Req = (C, t_c, \theta^{'})$, it does the following:
a) Check the freshness of t_c, then reject the request if t_c is not valid.
b) Compute $\theta = s_{AP}^{-1}\theta^{'}$ with its private key s_{AP}.
c) Compute $\theta_h = H_5(\theta)$
d) Extract $\sigma_c \| Q_c \| W_c \| m = C \oplus \theta_h$
e) Check the validity of $\langle \sigma_c, m \rangle$ and Verify $h_c \stackrel{?}{=} H_4(\sigma_c \| t_c, \theta)$ hold or not.
f) Extract $right \| ind_c = m$
g) Search client account indexed by ind_c. If it is, authorize the client; reject the session otherwise.
h) Choose $\tau \in \mathbb{Z}_P^*$ randomly, then compute $K = \tau\theta$ and $\psi = \tau P$
i) Compute the session key $key = H_4(h_c, K)$.
j) Compute $MAC_{key}(h_c)$ as the reply.
k) Send $MAC_{key}(h_c)$ and ψ to client as reply for service request.

When the client receives the reply from the AP, it computes $K = \alpha\psi$ and the session key $key = H_4(h_c, K)$. Then, it checks the integrity of $MAC_{key}(h_c)$ with session key key. Client will ignore the current session if the check produces a negative result. Otherwise, it authenticates the AP and uses the key with the AP in future communications. In Fig. 2, the phases of proposed HRAAP are described.

VIII. Analysis of HRAAP

This section is comprised of two subsections: the first part describes the security analysis, whereas the second subsection talks about the quantitative performance analysis.

A. Security Analysis

This subsection presents the security analysis of HRAAP in terms of security properties, which are countermeasures to the security threats presented in Section V-B as follows:

Theorem 2 (Client Anonymity): client anonymity in HRAAP means that except the requesting WBANs client and the requested AP, no one is able to reveal the real identity of the requesting WBANs client based on the existing communication, including the NM.

Proof: an ind_c is used in the HRAAP to identify the WBANs client. The computation of $ind_c = H_4(right, PK_c)$ requires the knowledge of $right$, and NM uses a secure channel to send both ind_c to SP and $right$ to WBANs client. Thus, it is impossible for an outsider to compute ind_c of client. In addition, the ind_c of the requesting client is only involved in $Req = (C, t_c, \theta^{'})$. Any adversary who eavesdrops on communication channel between WBANs client and AP, and wants to reveal ind_c of the client faces the decrypt operation to solve ECDLP (Elliptic Curve Discrete Logarithm Problem). In this way, only the requested AP can obtain the ind_c of WBANs client with the knowledge of its secret key. Thus, the proposed HRAAP resists the anonymity attack.

Theorem 3 (Unlinkability): unlinkability means that any of the adversaries $\mathcal{A}_I$ and $\mathcal{A}_{II}$ cannot distinguish WBANs clients based on their communication. In other words, any of the adversaries cannot link two different service requests to the same WBANs client.

Proof: it is assumed that, two different requesting messages are issued from the same WBANs client as follows:

- $Req_i = (C_i, t_i, \theta_i^{'})$, where $\theta_i^{'} = \alpha_i PK_{AP}$ and C_i is a ciphertext generated by θ_i.
- $Req_j = (C_j, t_j, \theta_j^{'})$, where $\theta_j^{'} = \alpha_j PK_{AP}$ and C_j is a ciphertext generated by θ_j.

It is clear that, the adversaries $(\mathcal{A}_I, \mathcal{A}_{II})$ are unable to link the two requests (Req_i, Req_j) due to the usage of two different random values $\alpha_i, \alpha_j \in \mathbb{Z}_p^*$. In other words, the two requests are independent since the ciphertext (C_i, C_j) and the parameters $(\theta_i^{'}, \theta_j^{'},)$ are generated by using two different random numbers. As a result, the proposed HRAAP withstands the linkability attack.

Theorem 4 (Non-repudiation): after successful authentication,

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

the WBANs client cannot deny that he/she has accessed the service supplied by the AP

Proof: a WBANs client can only generate a legal signature tuple of (h_c, β_c, μ_c), which includes the client index ind_c. According to lemmas 1 and 2, even the NM cannot impersonate the WBANs client to sign such a valid signature. Thus, the proposed HRAAP resists the repudiation attack.

Theorem 5 (Replay Attack Resilience): the proposed HRAAP achieves the replay attack resilience property

Proof: when the AP receives a request from WBANs client, it will check the freshness of t_c before executing other steps, where t_c is current time stamp. In this situation, the AP can find the replay attack easily. Besides, WBANs client can also find the replay attack of a response message by checking the correctness of $MAC_{key}(h_c)$ to know which key is generated by using random value $\alpha \in \mathbb{Z}_p^*$, which is selected by WBANs client in each session. Therefore, the proposed HRAAP withstands the replay attack.

Theorem 6 (Mutual Authentication): in the proposed HRAAP, the requested AP authenticates accessing WBANs client, with the requesting WBANs client authenticating a requested AP at the same time.

Proof: the requested AP authenticates the requesting WBANs client by checking the client's signature (σ_c, m), which resists both adversaries $\mathcal{A}_I$ and $\mathcal{A}_{II}$. The security proof is presented in lemma 1 and lemma 2, respectively (see appendix A and B for security proof). Moreover, the requested AP checks the validity of h_c with the result calculated by him/herself, which contains θ_c, since AP is the only one who can recover θ_c from $\theta_c^{'}$ by using its secret key, and then check $h_c \stackrel{?}{=} H_4(\sigma_c \| t_c, \theta)$. Furthermore, the client ind_c is another shared secret value between client and AP, which gives more strength for requested AP to authenticate the WBANs client. The requesting WBANs client authenticates the requested AP by verifying the integrity of $MAC_{key}(h_c)$ by using the calculated session key key, which depends on two random numbers $\alpha, \tau \in \mathbb{Z}_p^*$. If the client receives a right $MAC_{key}(h_c)$, then the AP is the correct one and the WBANs client wants to access for service. Hence, the proposed HRAAP resists the impersonation attack.

Theorem 7 (Forward Security): the security property is modeled as: if the adversary reveals a secret key of both WBANs client and AP, the previous session keys established will not be compromised.

Proof: it is assumed that an adversary compromises the full private key of WBANs client and the secret key of AP, after establishing a shared session key between them. In addition, an adversary eavesdrops on a request coming from client and the service response coming from AP, both client and AP compute $K = \alpha\tau P$, then compute the session key $key = H_4(h_c, K)$. However, an adversary still faces the problem to compute $\tau\theta$ or $\alpha\psi$ from $(\theta^{'}, \psi)$, both of which require the adversary to solve CDHP in $\mathbb{G}_1$ with non-negligible advantages. Thus, the proposed HRAAP inherits the forward security property.

Theorem 8 (Immunity of Key Escrow): in the HRAAP, the malicious NM is unable to impersonate the WBANs client or AP without being discovered

Proof: in the proposed HRAAP, the WBANs clients are constructed based on CL-PKC (Certificateless Public Key Cryptosystem) domain that can solve the inherent key escrow problem in ID-PKC (Identity based Public Key Cryptosystem). And the AP is constructed based on PKC (Public Key Cryptography) domain that does not have key escrow problem. In other words, according to lemmas 1 and 2, the malicious NM cannot impersonate the WBANs client since the client generates its full-private key by itself by using secret value x_c. And the fact is that AP generates its secret key means that it is not available to the NM. Therefore, the proposed HRAAP achieves the property.

Theorem 9 (Session Key Establishment): after successful authentication between requesting WBANs client and requested AP, both sides establish a shared session key.

Proof: it is observed that the requested AP can only recover θ from $\theta^{'}$, then compute $K = \tau\theta$ and session key $key = H_4(h_c, K)$. On the other hand, the requesting WBANs client can only check the integrity of $MAC_{key}(h_c)$, after computing $K = \alpha\psi$ and session key $key = H_4(h_c, K)$. key is only shared by WBANs client and AP. Therefore, the proposed HRAAP can provide the session key establishment property and explicit key confirmation property as well.

Theorem 10 (Non Key Control): this property is modeled as, neither one of WBANs client nor AP forces the session key key to be the preselected value.

Proof: in the proposed HRAAP, both the WBANs client and AP compute the session key $key = H_4(h_c, K)$, where $K = \alpha\tau P$. Neither of WBANs client and AP can predetermine the session key since it is impossible for the AP to find $\alpha \in \mathbb{Z}_p^*$ selected by the WBANs client. On the other hand, it is impossible for WBANs client to find $\tau \in \mathbb{Z}_p^*$ selected by AP. Therefore, the proposed HRAAP achieves the property.

B. Quantitative Performance Analysis

This subsection is made up of two parts: the first part talks about the advantages of the proposed HRAAP in terms of computational cost, whereas the second part describes the advantages of the proposed HRAAP in terms of energy consumption. It should be noted that only the WBANs client is considered since it is resource limited.

1) Computational Cost: in this part, an efficient comparison between the proposed HRAAP and those of the existing related schemes proposed by Liu et al. [45], Xiong. [46], Wang and Zhang [48], and He et al. [49] have been given in terms of computational cost and domains. This is shown in Table II. For computational cost, only paring operation, exponentiation in $\mathbb{G}_2$ and point multiplication in $\mathbb{G}_1$ are considered. Here, the cost of arithmetic operations and hash functions are ignored, as they are relatively negligible compared to the above three

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

operations. In Table II, P, PM, E and $|\bullet|$ represent a pairing computation in $\mathbb{G}_2$, a point multiplication in $\mathbb{G}_1$, an exponentiation in $\mathbb{G}_2$ and the size of "$\bullet$"in byte, respectively. From Table II, it is observed that the proposed HRAAP only requires three points multiplication in WBANs client. In addition, it is a heterogeneous protocol that allows WBANs client in CL-PKC domain to send a message to AP in PKC domain.

From Table II, it is clear that the ECC-based is required only in Xiong's scheme [46] and the pairing-based is required in the other four schemes. To achieve good performance for ECC-based, Koblitz curve $E : y^2 = x^3 + ax^2 + b$ [53], which is defined over binary field by [54], is used. The scalar multiplication is faster in this curve due to the use of "wTNAF"method [55]. According to the experimental results in [56], to achieve 80-bit security level the ECC-based scalar multiplication on the Koblitz curve, which is defined over $\mathbb{F}_{2^{163}}$ binary field needs 0.32 s on ATmega128L-based platform. To achieve the same security level at 80-bit for pairing-based, the supersingular curve $E : y^2 + y = x^3 + x$, which is defined over $\mathbb{F}_{2^{271}}$ field with an embedding degree of 4 is used. In this curve, the Eta pairing $\eta_T : E(\mathbb{F}_{2^{271}}) \times E(\mathbb{F}_{2^{271}}) \rightarrow \mathbb{F}_{2^{4.271}}$ is fastest at 80-bit security level [60]. According to the implementing results in [61] [62], the computation of η_T pairing takes 1.90 s and point multiplication needs 0.81 s for 80-bit security level on MICA2 built with an ATmega128 8-bit micro-controller based on the AVR architecture, 4KB RAM and 128KB of FLASH program memory (ROM). Also, Shim et al [65] has shown that the exponentiation operation requires 0.9 s. Now, the computation time on WBANs client of Liu et al. [45], Xiong. [46], Wang and Zhang [48], He et al. [49] and the proposed HRAAP are $4 \times 0.81 + 1 \times 0.9 = 4.14$ s, $10 \times 0.32 = 3.20$ s, $3 \times 0.81 + 1 \times 1.9 = 4.33$ s, $4 \times 0.81 = 3.24$ s, $3 \times 0.81 = 2.43$ s, respectively.

2) Energy consumption: in this part, an efficient comparison between the proposed HRAAP and those of the existing relevant schemes proposed by Liu et al. [45], Xiong. [46], Wang and Zhang [48], and He et al. [49], in terms of energy consumption are given. It is assumed that the MICA2 is set as simulation platform for WBANs client. The power level of MICA2 is 3.0 V, the transmitting current draw mode is 27 mA, the receiving current drawn mode is 10 mA, the current drawn in active mode is 8.0 mA and the data rate is 12.4 kbps [63]. The energy consumption for computation and communication is as follows:

- Energy for computation: for computation of energy, the equation $W = V \times I \times t$ is used, where W, V, I and t represent a consumption power in millijoules (mJ), power level of platform in volts, current draw in active mode in milliamps (mA) and the time in seconds (s), respectively [64]. As done in [65] [66], the energy consumption on WBANs client during computation process of Liu et al. [45], Xiong. [46], Wang and Zhang [48], He et al. [49] and proposed HRAAP are $3.0 \times 8.0 \times (4 \times 0.81 + 1 \times 0.9) = 99.36$ mJ, $3.0 \times 8.0 \times (10 \times 0.32) = 76.8$ mJ, $3.0 \times 8.0 \times (3 \times 0.81 + 1 \times 1.9) = 103.92$ mJ, $3.0 \times 8.0 \times (4 \times 0.81) = 77.76$ mJ and $3.0 \times 8.0 \times (3 \times 0.81) = 58.32$ mJ, respectively.
- Energy for communication: first, the message sizes made by different schemes are analyzed, since the size of message is directly related to the energy consumption on message propagation. It is assumed that the byte length of ID, $right$ and current time stamp t_c are set to 4, 8 and 2 bytes, respectively. In addition, It is supposed that the SHA256 is used for MAC.
  Message size: for Liu et al. [45], Wang and Zhang [48], He et al. [49] and the proposed HRAAP, the pairing-friendly supersingular curve defined over $\mathbb{F}_{2^{271}}$ binary field with 252-bits prime order and an embedding degree of 4 is used. In this curve, the size of element in $\mathbb{G}_1$ is 542-bits and the size of element in group $\mathbb{G}_2$ is 1084-bits (4x271). To reduce the communication overhead, the size of element in $\mathbb{G}_1$ can be compressed to 34 bytes since the x-coordinate and a single bit of y-coordinate have to be sent, and the receiver can easily derive y-coordinate using the curve equation [65]. The size of transmitting and receiving message of four schemes is as follows:
  - In the Liu et al. [45] scheme, the WBANs client sends a request message $\langle \upsilon, U, m, \sigma, t_c, T^{'} \rangle$ to AP, where, U, $T^{'} \in \mathbb{G}_1$, $\sigma \in \mathbb{G}_2$, $m \in \{|\{0,1\}^* + \mathbb{G}_2|\}$ and $\upsilon \in \mathbb{Z}_p^*$. And the AP responses $MAC_{key}(\upsilon)$ to client, where MAC is SHA256. Then, the client needs to transmit $|\mathbb{Z}_p^*| + 2|\mathbb{G}_1| + 2|\mathbb{G}_2| + |right| + |t_c| = 32 + 2 \times 34 + 2 \times 136 + 8 + 2 = 382$ bytes, and needs to receive $|MAC| = 32$ bytes.
  - In the Wang and Zhang [48] scheme, the WBANs client sends a request message $\langle R_c, T_c, Auth_c \rangle$ to AP, where $Auth_c \in \{|\{0,1\}^* + \{0,1\}^* + \mathbb{G}_1|\}$. And the AP responses $\langle R_{AP}, T_{AP}, Auth_{AP} \rangle$ to client, where $Auth_{AP} \in \mathbb{Z}_p^*$. Then, the client needs to transmit $|ID| + 2|\mathbb{G}_1| + 2|t_c| = 4 + 2 \times 34 + 2 \times 2 = 76$ bytes, and needs to receive $|MAC| + |\mathbb{G}_1| + |t_c| = 32 + 34 + 2 = 68$ bytes.
  - In the He et al. [49] scheme, the WBANs client sends a request message $\langle W, X, t_c \rangle$ to AP, where $W \in \{|\{0,1\}^* + \{0,1\}^* + \mathbb{G}_1|\}$. And the AP responses $\langle Y, Auth \rangle$ to client, where $Auth$ is SHA256. Then, the client needs to transmit $|ID| + 2|\mathbb{G}_1| + |right| + |t_c| = 4 + 2 \times 34 + 8 + 2 = 82$ bytes, and needs to receive $|MAC| + |\mathbb{G}_1| = 32 + 34 = 66$ bytes.
  - In the proposed HRAAP, the WBANs client sends a request message $\langle C, t_c, \theta^{'} \rangle$ to AP, where $C \in \{|\mathbb{Z}_p^* + \mathbb{Z}_p^* + \mathbb{G}_1 + \mathbb{G}_1 + \mathbb{G}_1 + \{0,1\}^* + \mathbb{Z}_p^*|\}$. And the AP responses $\langle MAC_{key}(h_c), \psi \rangle$ to client. Then, the client needs to transmit $3|\mathbb{Z}_p^*| + 4|\mathbb{G}_1| + |right| + |t_c| = 3 \times 32 + 4 \times 34 + 8 + 2 = 242$ bytes, and needs to receive $|MAC| + |\mathbb{G}_1| = 32 + 34 = 66$ bytes.

  For Xiong. [46] scheme, a Koblitz curve defined over $\mathbb{F}_{2^{163}}$ binary field with 163-bits prime order is used. In this curve, the size of element in $\mathbb{G}$ is 163-bit and can be compressed to 21 bytes. The size of transmitting and receiving message for [46] scheme is as follows:
  - The WBANs client sends a request message $\langle C_1, C_2 \rangle$ to AP, where $C_1 \in \mathbb{G}$ and $C_2 \in |\{0,1\}^* + 3\mathbb{G} + \{0,1\}^*|$. And the AP responses $\langle MAC_{key}(T_B), T_B \rangle$

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

TABLE II: Quantitative analysis of authentication schemes for WBANs client

Schemes	Computation cost		Communication cost		Domains	Curve type require
	Comp.offline	Comp.online	Transmit	Receive		
Liu et al. [45]	—	$4PM+1E$	$\|\mathbb{Z}_p^*\|+2\|\mathbb{G}_1\|+2\|\mathbb{G}_2\|+\|right\|+\|t_c\|$	$\|MAC\|$	CL-PKC → PKC	Pairing-based
Xiong. [46]	—	$10PM$	$\|ID\|+4\|\mathbb{G}\|+\|t_c\|$	$\|MAC\|+\|\mathbb{G}\|$	CL-PKC → CL-PKC	ECC-based
Wang and Zhang [48]	—	$3PM+1P$	$\|ID\|+2\|\mathbb{G}_1\|+2\|t_c\|$	$\|MAC\|+\|\mathbb{G}_1\|+\|t_c\|$	ID-PKC → ID-PKC	Pairing-based
He et al. [49]	—	$4PM$	$\|ID\|+2\|\mathbb{G}_1\|+\|right\|+\|t_c\|$	$\|MAC\|+\|\mathbb{G}_1\|$	CL-PKC → PKC	Pairing-based
Proposed HRAAP	$3PM+1E$	$3PM$	$3\|\mathbb{Z}_p^*\|+4\|\mathbb{G}_1\|+\|right\|+\|t_c\|$	$\|MAC\|+\|\mathbb{G}_1\|$	CL-PKC → PKC	Pairing-based

TABLE III: Comparison of authentication schemes in terms of computation overhead, communication overhead and energy consumption on MICA2

Schemes	Comp.overhead (s)	Comm.overhead (Byte)		Energy for comp	Energy for comm	Total energy (mJ)
		Transmit.overhead	Receive.overhead			
Liu et al. [45]	4.14	382	32	99.36	20.58	119.94
Xiong. [46]	3.20	90	53	76.80	5.72	82.52
Wang and Zhang [48]	4.33	76	68	103.92	5.29	109.21
He et al. [49]	3.24	82	66	77.76	5.56	83.32
Proposed HRAAP	2.43	242	66	58.32	13.93	72.25

to client. Then, the client needs to transmit $|ID|+4|\mathbb{G}|+|t_c|=4+4\times21+2=90$ bytes, and needs to receive $|MAC|+|\mathbb{G}|=32+21=53$ bytes.

For energy consumption of request/response message, the equation $W=V\times I\times x\times\frac{8}{d}$ is used, where I,x and d represent the current draw in transmitting/receiving mode, size of data in bytes and platform data rate, respectively [64]. The energy consumption on WBANs during sending a request message for Liu et al. [45], Xiong. [46], Wang and Zhang [48], He et al. [49] and the proposed HRAAP are $3.0\times27\times382\times\frac{8}{12400}=19.96$ mJ, $3.0\times27\times90\times\frac{8}{12400}=4.70$ mJ, $3.0\times27\times76\times\frac{8}{12400}=3.97$ mJ, $3.0\times27\times82\times\frac{8}{12400}=4.28$ mJ and $3.0\times27\times242\times\frac{8}{12400}=12.65$ mJ, respectively. And the energy consumption on WBANs during receiving a response message for Liu et al. [45], Xiong. [46], Wang and Zhang [48], He et al. [49] and the proposed HRAAP are $3.0\times10\times32\times\frac{8}{12400}=0.62$ mJ, $3.0\times10\times53\times\frac{8}{12400}=1.02$ mJ, $3.0\times10\times68\times\frac{8}{12400}=1.32$ mJ, $3.0\times10\times66\times\frac{8}{12400}=1.28$ mJ and $3.0\times10\times66\times\frac{8}{12400}=1.28$ mJ, respectively. As is observed from Table III, the proposed HRAAP is the most efficient in terms of computation overhead and energy consumption among the four schemes.

Fig. 3 and Fig. 4 depict the computation overhead and energy consumption, respectively on WBANs client when the number of the requested APs increases. As is seen from Fig. 3 and Fig. 4, the proposed HRAAP achieves less computational time as well as energy consumption compared with four relevant anonymous authenticated key schemes. As a result, a heterogeneous scheme that comprises of CL-PKC (for WBANs domain) and PKC (for AP domain) will be better for Internet of Things applications.

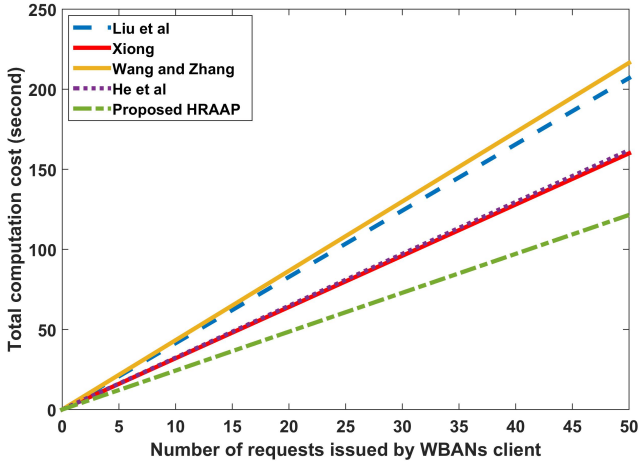

Fig. 3: The computation cost of WBANs client regarding number of requests

IX. Application Scenario

As the focus of this paper is on designing a secure schemes to provide security for Healthcare application in IoTs, this section gives an application scenario for secure data transmission between WBANs client and AP in the IoTs using the proposed HRAAP. In this scenario, it is presumed that, the sensor nodes or wearable devices attached to the patients' body gathers the patients' data and sends it to the local server in short range of WBANs. For communication between wearable devices and local server, the standard IEEE 802.15.6 can be used, which is developed for low power device communication and operation on, in or around the human body to serve a variety of applications. Then the local server transmits the data to the AP (Application Provider) via an Internet medium. Finally, the physicians can login to the patients' data stored in the AP via the Intranet/Internet. Since most devices are wireless in nature, an adversary may gain some critical information of a patient or track a particular patient by linking two or more messages to the same sensor node of the patient. This information can help the adversary to launch physical attacks against this patient. Therefore, the patients' data sent from the WBANs to the AP must be secure in order to ensure the correctness of information. It should be noted that, this application is only focused on remote anonymous authentication and session key establishment between WBANs client and AP.

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

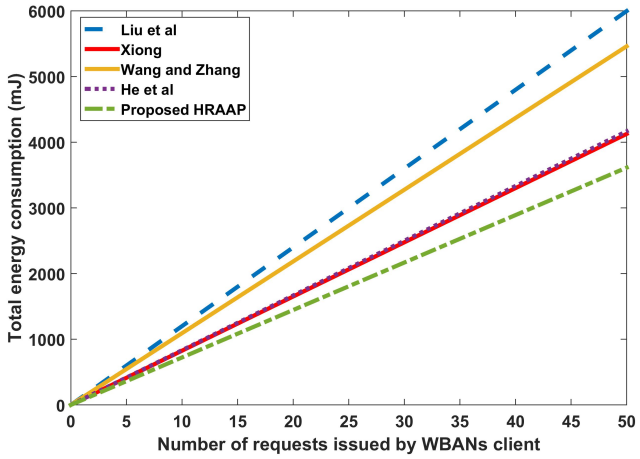

Fig. 4: The energy consumption of WBANs client regarding number of requests

1) Framework Model: this model comprises of four main entities: MN (Network Manager), WBANs, local servers and AP. Fig. 5 shows a secure framework model for secure data transmission between WBANs clients and AP in the IoTs using the proposed HRAAP.

- NM: it is in charge of generating a system $params$ and partial private key for WBANs clients in CL-PKC domain. First, it runs the setup algorithm to get system $params$, then sends the system $params$ to WBANs clients and the AP. Moreover, NM receives the client's public key (PK_c), then runs partial private key algorithm to generate a partial key D_c of client, and transmits it to the client in a secure channel. In addition, it computes clients' indexes, then sends them to AP in a secure channel such as SSL (Secure Socket Layer).
- WBANs: it is comprised of clients (sensor nodes) and local servers. The communication between clients and local servers is assumed to be based on standard IEEE 802.15.6 [74].
- WBANs client: it has two tasks as follows:
  1) It takes system $params$ from NM, then runs public key algorithm to obtain its secret value x_c and public key PK_c. Then, it transmits the public key to the NM.
  2) It gets its partial private key from NM, then computes its full private key.

  It should be noted that, the WBANs client is preloaded with the precomputed value $\sigma_c^{'}$ as an Offsign algorithm result, system $params$ and a group of PK_{AP} for different APs of interest.
- Local Server: it sends the data coming from WBANs client to the AP and vice-versa.
- AP: it gets system $params$ from NM, then it generates its private/public key. In addition, it transmits its public key PK_{AP} to NM.
- Database: it stores WBANs clients' indexes and patients' data.
- Backup Server: it uses for data backup.

For authentication and session key establishment, the WBANs client sends a service request $Req = (C, t_c, \theta^{'})$ to local server. The local server transmits a service request to the AP. When the AP receives the request $Req = (C, t_c, \theta^{'})$, it checks the validity. If it is valid, it computes a session key key, then uses a session key key to compute a MAC and sends it back to WBANs client. The WBANs client computes a session key key, then checks the integrity of MAC by using a computed session key key. Finally, the session key key is used for future communication between WBANs client and AP. As is seen, this framework can achieve remote anonymous authentication and session key establishment between WBANs client and AP. Moreover, only less computation is done in the WBANs client since all heavy computation is taken away from the online phase. As a result, the proposed HRAAP is feasible for IoTs applications.

X. Conclusion and Future Work

In this paper, a lightweight online/offline certificateless signature scheme is first proposed and proved to be secure in random oracle model. Then, based on a novel proposed signature, a heterogeneous remote anonymous authentication and session key establishment protocol is proposed to assist anonymously secure data transmission from WBANs to AP via an Internet medium. A theoretical security analysis, as well as computation time and energy consumption are given in detail, which show that the proposed HRAAP achieves strong security and offers less time as well as less energy consumption among the efficient existing relevant work. In addition, in the proposed HRAAP, the WBANs client belongs to CL-PKC and AP belongs to PKC, which make it more scalable at Internet side. Furthermore, an application scenario is given to demonstrate how the proposed HRAAP can be applied in the IoTs. The future work will focus on roaming users and sending data to more than one server in different layers.

Appendix A
Proof of Lemma 1

As is similar to the proof in [71] [70], it is assumed that an algorithm $\mathcal{C}$ takes as input (q+1)-tuple $(P, \alpha P, \alpha^2 P, \alpha^3 P, ..., \alpha^q P)$ and attempts to produce a pair $(\lambda, \frac{1}{\lambda+\alpha} P)$ after interacting with $\mathcal{A}_{II}$. Here λ, $\alpha \in \mathbb{Z}_p^*$.

First, the input with consistent view to answer the adversary queries is shown. Then the forking lemma [73] is applied to complete the security proof.

Initial: an algorithm $\mathcal{C}$ takes (q+1)-tuple $(P, \alpha P, \alpha^2 P, \alpha^3 P, ..., \alpha^q P)$ as input and selects $\lambda_1, \lambda_2, ..., \lambda_{q-1} \in \mathbb{Z}_p^*$ randomly. Then it sets up a generator Q and the public key $Q_{pub} = \alpha Q$ both parameters in $\mathbb{G}_1$, such that it knows q-1 pairs $(\lambda_c, \frac{1}{\lambda_c+\alpha} Q)$ for $c \in \{1, ..., q-1\}$ as in [72]. To do so, let $f(z)$ be the polynomial $f(z) = \prod_{c=1}^{q-1}(z + \lambda_c)$ and expand f(z) to obtain $f(z) = \sum_{c=0}^{q-1} \tau_c z^c$, where $\tau_0, \tau_1, ..., \tau_{q-1} \in \mathbb{Z}_p^*$. Then compute

- A generator $Q = \sum_{c=0}^{q-1} \tau_c(\alpha^c P) = f(\alpha)P \in \mathbb{G}_1$

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

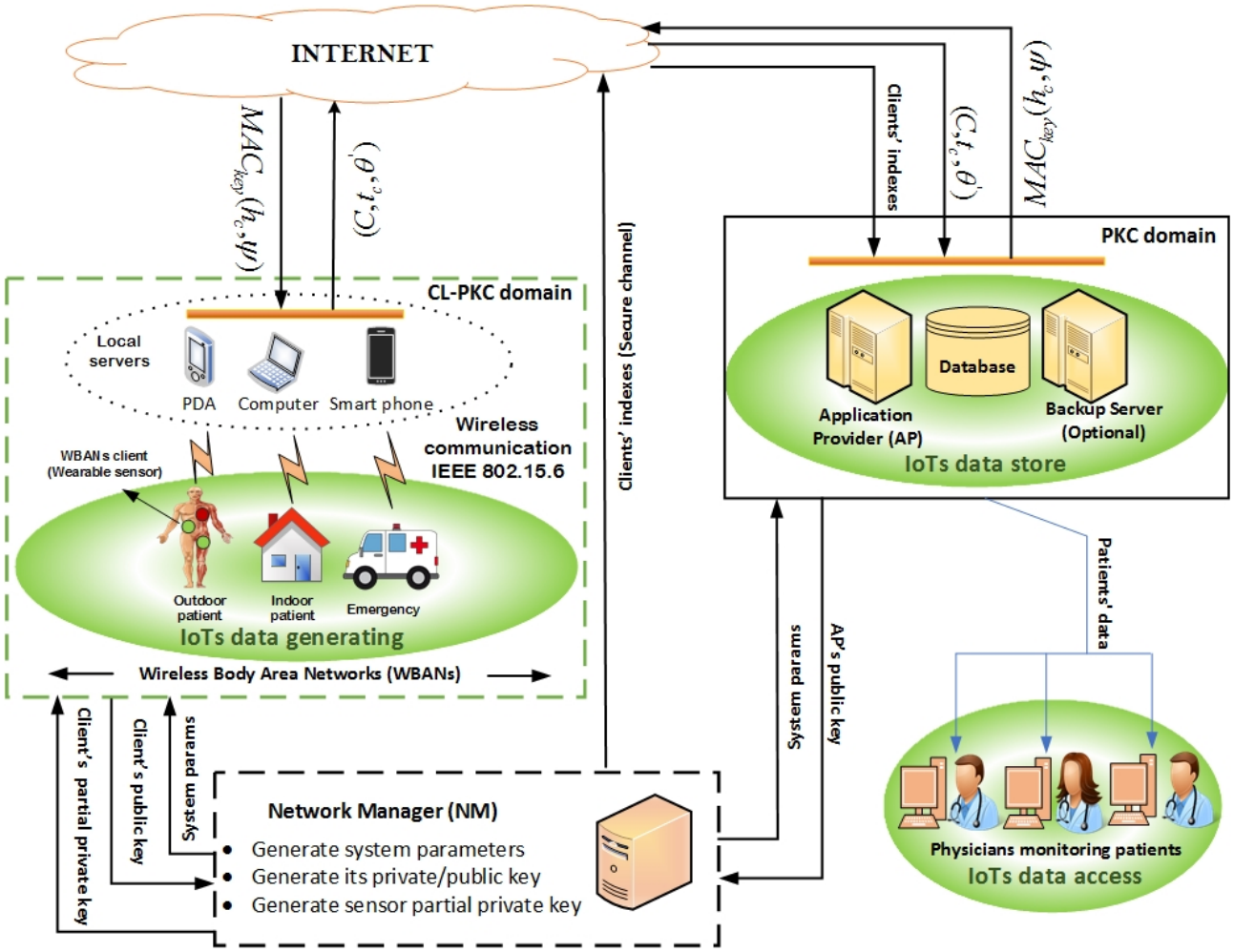

Fig. 5: A secure framework model for data transmission between WBANs client and application provider in the IoTs

- The public key $Q_{pub} = \sum_{c=1}^{q} \tau_{c-1}(\alpha^c P) = \alpha f(\alpha) P = \alpha Q \in \mathbb{G}_1$. It should be noted that an algorithm C does not know the α.

Next, to obtain $(\lambda_c, \frac{1}{\lambda_c+\alpha}Q)$ for each $c = 1, ..., q-1$ and let $f_c(z)$ be the polynomial $f_c(z) = f(z)/(z+\lambda_c) = \prod_{j=0, j\neq c}^{q-1} d_j z^j$. As is done before, an algorithm $\mathcal{C}$ expands $f_c(z)$ to be written as $f_c(z) = \sum_{j=0}^{q-2} d_j z^j$. Then compute

- $\sum_{j=0}^{q-2} d_j \alpha^j P = f_c(\alpha) P = \frac{f(\alpha)}{\lambda_c+\alpha} P = \frac{1}{\lambda_c+\alpha} Q \in \mathbb{G}_1$.

As a result, the pairs $(\lambda_c, \frac{1}{\lambda_c+\alpha}Q)$ can be computed using the left side in the above equation.

Now, the challenger $\mathcal{C}$ is ready to answer an adversary $\mathcal{A}_I$ queries in EUF-CMA-I game. It runs $\mathcal{A}_I$ as subroutine and simulates its attacks environment as follows:

$\mathcal{C}$ sends $\mathcal{A}_I$ system parameters $params$ such that Q is a group generator, $Q_{pub} = \alpha Q$ is a public key and $g = \hat{e}(Q, Q)$. Moreover, C picks $ID_c^* \in \{0,1\}^*$ as challenge identity, and sends it to $\mathcal{A}_I$. Without loss of generality, it is assumed that, the queries to H_1 are distinguished, and $\mathcal{A}_I$ should perform $H_1(ID)$ query before ID is used. Moreover, the public key query has previously been made before partial private query on that identity. To avoid collision and be consistently respond to these queries, $\mathcal{C}$ creates three lists L_{H_1}, L_{H_2} and L_{pk}, which are initially empty. Furthermore, the target identity ID_c^* is asked H_1 query at some point. Then, $\mathcal{C}$ simulates the oracle queries of $\mathcal{A}_I$ as follows:

- H_1 queries: for query on input $H_1(ID_c)$. $\mathcal{C}$ scans whether a tuple $(ID_c, h_{1,c})$ is contained in L_{pk}. If it does, C returns $h_{1,c}$ to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ picks a random value $h_{1,c} \in \mathbb{Z}_p^*$ and returns it to $\mathcal{A}_I$. It then, adds $(ID_c, h_{1,c})$ to the L_{pk}.
- H_2 queries: for $\mathcal{A}_I$ query on input $H_2(PK_c)$. If $PK_c = PK_c^*$ $\mathcal{C}$ returns $\lambda_c^* \in \mathbb{Z}_p^*$ to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ acts as follows:
  $\mathcal{C}$ checks a L_{H_2} for a tuple (PK_c, λ_c). If it is so, $\mathcal{C}$ returns λ_c to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ picks $\lambda_c \in \mathbb{Z}_p^*$ and returns it to $\mathcal{A}_I$. Finally, $\mathcal{C}$ stores a tuple $(PK_c, \lambda_c or \lambda_c^*)$ in a list L_{H_2}.
- Request Public-Key queries: when $\mathcal{A}_I$ makes this query on input (ID_c) and $\mathcal{C}$ checks L_{pk} list to see whether a tuple (ID_c, PK_c) is defined. If it does, $\mathcal{C}$ returns PK_c to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ performs as follows:
  $\mathcal{C}$ checks L_{H_1} list to see whether a tuple $(ID_c, h_{1,c})$ is contained. If it is, it recovers $h_{1,c}$ value and picks $x_c \in \mathbb{Z}_P^*$ randomly ($\mathcal{C}$ may need to perform H_1 query). Then, it sets $PK_c = x_c h_{1,c} P$. Finally, $\mathcal{C}$ returns PK_c to $\mathcal{A}_I$ and adds the tuple (ID_c, PK_c, x_c) to the L_{pk} list.

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

- Request Partial-Private-Key queries: $\mathcal{A}_I$ may ask a partial-private key query. When $\mathcal{A}_I$ performs this query on ID_c, if $ID_c = ID_c^*$, $\mathcal{C}$ outputs "failure" and halts. Otherwise, $\mathcal{C}$ works as follows: $\mathcal{C}$ checks a list L_{H_2} to see whether a tuple (PK_c, λ_c) has already existed. If it is, $\mathcal{C}$ sets $D_c = \frac{1}{\lambda_c+\alpha}Q$ and sends it to $\mathcal{A}_I$. Otherwise, $\mathcal{C}$ needs to perform public key and H_2 queries, then simulate as above process and sends D_c to $\mathcal{A}_I$.
- Request Full-Private-Key queries: when $\mathcal{A}_I$ extracts full-private key query for identity ID_c, if $ID_c = ID_c^*$, $\mathcal{C}$ returns "failure"and stops. Otherwise, $\mathcal{C}$ recovers the value x_c from L_{pk} list ($\mathcal{C}$ may need to perform a public key query for identity ID_c), and it knows the partial-private key of ID_c ($D_c = \frac{1}{\lambda_c+\alpha}Q$). Then, $\mathcal{C}$ sets $SK_c = (x_c)^{-1}(D_c)$ and returns it to $\mathcal{A}_I$.
- Replace Public-Key queries: when $\mathcal{A}_I$ makes this query on $(ID_c, PK_c^{'})$, $\mathcal{C}$ scans whether the tuple (ID_c, PK_c, x_c) corresponding to ID_c is contained in the L_{pk}. If it is, $\mathcal{C}$ sets $PK_c = PK_c^{'}$ and $x_c = \perp$, then updates the corresponding information in a list L_{pk}, where $\perp$ denotes an unknown value. Otherwise, $\mathcal{C}$ makes a public key query, then simulates as above process.
- Signing Oracle queries: $\mathcal{A}_I$ may ask a signature query on (ID_c, m) for $c \in \{1, 2, 3, ..., q_{H_1}\}$. If $ID_c = ID_c^*$, $\mathcal{C}$ returns "failure" and halts. Otherwise, $\mathcal{C}$ picks $\mu_c \in \mathbb{G}_1$, $h_c, \beta_c \in \mathbb{Z}_p^*$ and recovers x_c value from L_{pk} list corresponding to ID_c. Then, it computes $\Gamma = \hat{e}(\beta_c\mu_c, Q_c + W_c)g^{-h_c}$, where $Q_c = x_c h_{2,c} Q$ and $W_c = x_c Q_{pub}$ (It should be noted that, $h_{2,c}$ is already defined in L_{H_2} list). And $\mathcal{C}$ patches the hash value $H_3 = (m, \Gamma)$ to $h_c \in \mathbb{Z}_p^*$. It should be noted that, $\mathcal{C}$ fails if the $H_3 = (m, \Gamma)$ has already been defined. But it only happens with probability $(q_{sig} + q_{H_3})/2^k$. Finally, $\mathcal{C}$ returns $\sigma_c = \langle h_c, \beta_c, \mu_c \rangle$, Q_c, W_c, and m to $\mathcal{A}_I$.

Next, it needs to be shown that the L-OOCLS scheme satisfies the forking lemma conditions [73] as follows. Through signing oracle queries of a message m, the tuple $\langle m, \Gamma, h_c, \beta_c, \mu_c \rangle$ is created, which is equivalent to the three-pass honest-verifier zero-knowledge protocol. Accordingly, a signature of a message m is a triple (σ_1, h, σ_2), where $\sigma_1 = \Gamma$, $h = (m, \Gamma)$ and $\sigma_2 = \beta_c\mu_c$, if the tuple $(\Gamma, h_c, \beta_c, \mu_c)$ can be simulated without the knowledge of the signer's private key. If $\mathcal{A}_I$ is really forged, then there exists another Turing machine $\mathcal{A}_I^{'}$, which has control over $\mathcal{A}_I$ to produce two valid signed messages $(m, \Gamma, h_c, \beta_c, \mu_c)$ and $(m, \Gamma, h_c^{'}, \beta_c^{'}, \mu_c^{'})$ for the same identity ID_c, such that $h_c \neq h_c^{'}$.

Lastly, the simulator $\mathcal{C}$ runs $\mathcal{A}_I^{'}$ controlled by $\mathcal{A}_I$ to produce two forgeries $(m^*, \Gamma^*, h_c^*, \beta_c^*, \mu_c^*)$ and $(m^*, \Gamma^*, h_c^{*'}, \beta_c^{*'}, \mu_c^{*'})$ corresponding to an identity ID_c^* for the same commitment Γ^* and a message m^*. If the two signatures are valid, then the following relation is obtained:

$$h_c^* = H_3(m, \hat{e}(\beta_c^*\mu_c^*, Q_c^* + W_c^*)g^{-h_c^*}) = H_3(m, \hat{e}(\beta_c^{*'}\mu_c^{*'}, Q_c^* + W_c^*)g^{-h_c^{*'}})$$

Then, it is drawn that

$$\hat{e}(\beta_c^*\mu_c^*, Q_c^* + W_c^*)g^{-h_c^*}) = \hat{e}(\beta_c^{*'}\mu_c^{*'}, Q_c^* + W_c^*)g^{-h_c^{*'}}$$

Also, it is deduced that

$$((h_c^* - h_c^{*'})^{-1}(\beta_c^*\mu_c^* - \beta_c^{*'}\mu_c^{*'}), Q_c^* + W_c^*) = g$$

$\mathcal{C}$ computes

$$\chi^* = (h_c^* - h_c^{*'})^{-1}(\beta_c^*\mu_c^* - \beta_c^{*'}\mu_c^{*'}) = \frac{1}{\lambda_c^*+\alpha}Q = \frac{f(\alpha)}{\lambda_c^*+\alpha}P$$

As in [72], by using long division, the polynomial f can be written as $f(z) = \upsilon(z)(z + \lambda_c^*) + \upsilon_{-1}$ for some polynomial $\upsilon(z) = \sum_{c=0}^{q-2} \upsilon_c z^c$ and some $\upsilon_{-1} \in \mathbb{Z}_p^*$. As a result, the polynomial $f(z)/(z + \lambda_c^*)$ can be written as:

$$\frac{f(z)}{(z + \lambda_c^*)} = \sum_{c=0}^{q-2} \upsilon_c z^c + \frac{\upsilon_{-1}}{z + \lambda_c^*}$$

Then it deduced that, $\frac{1}{\lambda_c^*+\alpha}P = \frac{1}{\upsilon_{-1}}(\chi^* - \sum_{c=0}^{q-2} \upsilon_c(\alpha^c P))$

$\mathcal{C}$ outputs the pairs $(\lambda_c^*, \frac{1}{\lambda_c^*+\alpha}P)$ as the solution to the q-SDH instance.

Finally, from the forking lemma, if $\mathcal{A}_I$ is able to forge a signature in a time t with probability $\epsilon \geq 10(q_{sig} + 1)(q_{sig} + q_{H_3})/2^k$, then a $t^{'}$-algorithm $\mathcal{C}$ can solve the q-SDH assumption within the expected time

$$t^{'} \leq 120686 q_{H_3} \frac{(t + O(q_{sig} t_p))}{\epsilon(1 - 1/2^k)(1 - q/2^k)} + O(q^2 t_{sm})$$

APPENDIX B
PROOF OF LEMMA 2

It is assumed that an algorithm C takes as input a Inv-CDHP instance $(P, x_c P)$ for random chosen $x_c \in \mathbb{Z}_p^*$ and $P \in \mathbb{G}_1$. Its goal is to compute $x_c^{-1}P$ from its interaction with $\mathcal{A}_{II}$. $\mathcal{C}$ runs $\mathcal{A}_{II}$ as subroutine and simulates its attacks environment as follows:

Initial: $\mathcal{C}$ picks $s \in \mathbb{Z}_p^*$ randomly and sets $PK = sP$, where s is the master key and PK is the public key. $\mathcal{C}$ gives both master key and system $params$ including public key to $\mathcal{A}_{II}$. Without loss of generality, it is assumed that, the queries to H_1 are distinguished, and the adversary $\mathcal{A}_{II}$ must perform $H_1(ID)$ query before ID is used. In addition, the public key query has previously been asked before partial private query on that identity. To avoid collision and be consistent for these answers queries, $\mathcal{C}$ maintains three lists L_{H_1}, L_{H_2} and L_{pk}, which are initially empty. Moreover, the target identity ID_c^* is asked H_1 query at some point. $\mathcal{C}$ then answers the oracle queries of $\mathcal{A}_{II}$ as follows:

- H_1 queries: when $\mathcal{A}_{II}$ makes this query for the input $H_1(ID_c)$, $\mathcal{C}$ checks whether a tuple $(ID_c, h_{1,c})$ is previously defined in L_{pk}. If so, C returns $h_{1,c}$ to $\mathcal{A}_{II}$. Otherwise, $\mathcal{C}$ picks a random value $h_{1,c} \in \mathbb{Z}_p^*$ and returns it to $\mathcal{A}_{II}$. It then, stores $(ID_c, h_{1,c})$ to the L_{pk}.
- H_2 queries: for query on input $H_2(PK_c)$. If $PK_c = PK_c^*$ $\mathcal{C}$ outputs $\lambda_c^* \in \mathbb{Z}_p^*$ to $\mathcal{A}_{II}$. Otherwise, $\mathcal{C}$ performs as follows:
  $\mathcal{C}$ scans a L_{H_2} for a tuple (PK_c, λ_c). If it does, $\mathcal{C}$ returns λ_c to $\mathcal{A}_{II}$. Otherwise $\mathcal{C}$ picks $\lambda_c \in \mathbb{Z}_p^*$ randomly and returns it to $\mathcal{A}_{II}$. Finally, $\mathcal{C}$ adds a tuple $(PK_c, \lambda_c or \lambda_c^*)$ in a list L_{H_2}.

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

- Request Public-Key queries: an adversary $\mathcal{A}_{II}$ may perform a public key query for identity ID_c, $\mathcal{C}$ checks L_{pk} list to know whether a tuple (ID_c, PK_c) is contained. If so, $\mathcal{C}$ returns PK_c to $\mathcal{A}_{II}$. Otherwise, $\mathcal{C}$ acts as follows: $\mathcal{C}$ scans L_{H_1} list to know whether a tuple $(ID_c, h_{1,c})$ is defined. If so, it recovers $h_{1,c}$ value and picks $x_c \in \mathbb{Z}_P^*$ randomly ($\mathcal{C}$ may need to ask H_1 query). Then, it sets $PK_c = x_c h_{1,c} P$. Finally, $\mathcal{C}$ returns PK_c to $\mathcal{A}_{II}$ and stores the tuple (ID_c, PK_c, x_c) to the L_{pk} list.
- Request Full-Private-Key queries: when $\mathcal{A}_{II}$ asks to extract full-private key query for identity ID_c. If $ID_c = ID_c^*$, $\mathcal{C}$ returns "failure"and halts. Otherwise, $\mathcal{C}$ retrieves the tuples (PK_c, λ_c) and (ID_c, PK_c, x_c) from the lists L_{H_2} and L_{pk}, respectively ($\mathcal{C}$ may need to ask a public key query for identity ID_c). And it sets $SK_c = (x_c)^{-1} \frac{1}{\lambda_c + s} P$, then returns it to $\mathcal{A}_{II}$.
- Signing Oracle queries: when $\mathcal{A}_{II}$ makes this query on (ID_c, m) for $c \in \{1, 2, 3, ..., q_{H_1}\}$. If $ID_c = ID_c^*$, $\mathcal{C}$ outputs "failure"and stops. Otherwise, $\mathcal{C}$ chooses $\mu_c \in \mathbb{G}_1$, $h_c, \beta_c \in \mathbb{Z}_p^*$ and retrieves x_c value from L_{pk} list corresponding to ID_c. Then it sets $\Gamma = \hat{e}(\beta_c \mu_c, Q_c + W_c) g^{-h_c}$, where $Q_c = x_c h_{2,c} P$ and $W_c = x_c P_{pub}$ (It is noted that, $h_{2,c}$ is already contained in L_{H_2} list). And $\mathcal{C}$ defines the hash function $H_3 = (m, \Gamma)$ to $h_c \in \mathbb{Z}_p^*$. It is noted that, $\mathcal{C}$ fails if the $H_3 = (m, \Gamma)$ has already been defined, but this only happens with probability $(q_{sig} + q_{H_3})/2^k$. Finally, $\mathcal{C}$ sends the signature $\sigma_c = \langle h_c, \beta_c, \mu_c \rangle$ with Q_c, W_c, and m to $\mathcal{A}_{II}$.

Now, the L-OOCLS scheme satisfies the forking lemma requirements [73] similar to the EUF-CMA-I game. It is observed that, the triples (σ_1, h, σ_2) can be simulated without knowing the private key. If $\mathcal{A}_{II}$ is really forged, then, there exists another Turing machine $\mathcal{A}_{II}^{'}$, which has control over $\mathcal{A}_{II}$ to output two valid signed messages $(m, \Gamma, h_c, \beta_c, \mu_c)$ and $(m, \Gamma, h_c^{'}, \beta_c^{'}, \mu_c^{'})$ for the same identity ID_c, such that $h_c \neq h_c^{'}$.

Lastly, the simulator $\mathcal{C}$ runs $\mathcal{A}_{II}^{'}$ controlled by $\mathcal{A}_{II}$ to output two forgeries $(m^*, \Gamma^*, h_c^*, \beta_c^*, \mu_c^*)$ and $(m^*, \Gamma^*, h_c^{*'}, \beta_c^{*'}, \mu_c^{*'})$ corresponding to an identity ID_c^* for the same commitment Γ^* and a message m^*. If the two signatures are valid, then the following relation is obtained:

$$h_c^* = H_3(m, \hat{e}(\beta_c^* \mu_c^*, Q_c^* + W_c^*) g^{-h_c^*}) = H_3(m, \hat{e}(\beta_c^{*'} \mu_c^{*'}, Q_c^* + W_c^*) g^{-h_c^{*'}})$$

Then, it is deduced that
$$\hat{e}(\beta_c^* \mu_c^*, Q_c^* + W_c^*) g^{-h_c^*}) = \hat{e}(\beta_c^{*'} \mu_c^{*'}, Q_c^* + W_c^*) g^{-h_c^{*'}}$$

Also, it is drawn that
$$((h_c^* - h_c^{*'})^{-1} (\beta_c^* \mu_c^* - \beta_c^{*'} \mu_c^{*'}), Q_c^* + W_c^*) = g$$

$\mathcal{C}$ computes
$$(h_c^* - h_c^{*'})^{-1} (\beta_c^* \mu_c^* - \beta_c^{*'} \mu_c^{*'}) = (x_c)^{-1} \frac{1}{\lambda_c^* + s} P$$

Let $\chi^* = (h_c^* - h_c^{*'})^{-1} (\beta_c^* \mu_c^* - \beta_c^{*'} \mu_c^{*'}) = (x_c)^{-1} \frac{1}{\lambda_c^* + s} P$

Then $(\lambda_c^* + s) \chi^* = (x_c)^{-1} P$

As a result, $\mathcal{C}$ outputs $(\lambda_c^* + s)\chi^*$ as the solution to the inv-ECDH instance $(P, x_c^{-1} P)$.

Finally, from the forking lemma, if $\mathcal{A}_{II}$ is able to forge a signature in a time t with probability $\epsilon \geq 10(q_{sig} + 1)(q_{sig} + q_{H_3})/2^k$, then a $t^{'}$-algorithm $\mathcal{C}$ can solve the inv-ECDH assumption within expected time

$$t^{'} \leq 120686 q_{H_3} \frac{(t + O(q_{sig} t_p))}{\epsilon(1 - 1/2^k)} + O(q^2 t_{sm})$$

ACKNOWLEDGMENT

This work was supported in part by Natural Science Foundation of China under Grant NSFC51677020, in part by China Postdoctoral Science Foundation under Grant 2015M572457, the Provincial Key Laboratory of power electronics energy saving technology and equipment(No.szjj2016-093) and 2018 Fundamental Research Funds for the Central Universities. The authors would like to thank EU CONHEALTH www.conhealth.eu for partialy founding this work. The authors would like to thank the associate editors and anonymous reviewers for their valuable feedback and insightful comments on the paper which helped us to improve its quality and presentation.

REFERENCES

[1] Links, Cees. "The Internet of Things will Change our World." ERCIM News 101.3 (2015): 76. https://ercim-news.ercim.eu/images/stories/EN101/ EN101-web.pdf
[2] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.
[3] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805. APA
[4] Latr, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. Wireless Networks, 17(1), 1-18.
[5] Varshney, Upkar. "Pervasive healthcare: applications, challenges and wireless solutions." Communications of the Association for Information Systems 16.1 (2005): 3.
[6] Seyedi, M., Kibret, B., Lai, D. T., & Faulkner, M. (2013). A survey on intrabody communications for body area network applications. IEEE Transactions on Biomedical Engineering, 60(8), 2067-2079.
[7] Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2011). Body area networks: A survey. Mobile networks and applications, 16(2), 171-193.
[8] Zhou, B., Hu, C., Wang, H., Guo, R., & Meng, M. Q. H. (2007, March). A wireless sensor network for pervasive medical supervision. In Integration Technology, 2007. ICIT'07. IEEE International Conference on (pp. 740-744). IEEE.
[9] Hanson, M. A., Powell Jr, H. C., Barth, A. T., Ringgenberg, K., Calhoun, B. H., Aylor, J. H., & Lach, J. (2009). Body area sensor networks: Challenges and opportunities. Computer, 42(1).
[10] Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless body area networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), 1658-1686.
[11] Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). RFC 4944: Transmission of IPv6 packets over IEEE 802.15.4 networks.
[12] Roman, R., & Lopez, J. (2009). Integrating wireless sensor networks and the internet: A security analysis. Internet Research, 19(2), 246-259.
[13] Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. IEEE Wireless communications, 17(1).
[14] Bhattarai, Sulabh, and Yong Wang. "End-to-End Trust and Security for Internet of Things Applications." Computer 4 (2018): 20-27.
[15] Alabady, S.A., Al-Turjman, F. and Din, S., 2018. A novel security model for cooperative virtual networks in the IoT era. International Journal of Parallel Programming, pp.1-16.

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

[16] Cherukuri, S., Venkatasubramanian, K. K., & Gupta, S. K. (2003, October). BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on (pp. 432-439). IEEE.

[17] Poon, Carmen CY, Yuan-Ting Zhang, and Shu-Di Bao. "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health."IEEE Communications Magazine44.4 (2006): 73-81.

[18] Zhang, Z., Wang, H., Vasilakos, A. V., & Fang, H. (2012). ECG-cryptography and authentication in body area networks.IEEE Transactions on Information Technology in Biomedicine,16(6), 1070-1078.

[19] Venkatasubramanian, Krishna K., Ayan Banerjee, and Sandeep Kumar S. Gupta. "PSKA: Usable and secure key agreement scheme for body area networks."IEEE Transactions on Information Technology in Biomedicine14.1 (2010): 60-68.

[20] Zeng, Kai, Kannan Govindan, and Prasant Mohapatra. "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]."IEEE Wireless Communications17.5 (2010).

[21] L. Cai, K. Zeng, H. Chen, and P. Mohapatra, Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas, in Network and Distributed System Security Symposium, 2011, pp. 1-20.

[22] Shi, L., Yuan, J., Yu, S., & Li, M. (2013, April). ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks. InProceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks(pp. 155-166). ACM.

[23] Kalamandeen, A., Scannell, A., de Lara, E., Sheth, A., & LaMarca, A. (2010, June). Ensemble: cooperative proximity-based authentication. InProceedings of the 8th international conference on Mobile systems, applications, and services(pp. 331-344). ACM.

[24] Mathur, S., Miller, R., Varshavsky, A., Trappe, W., & Mandayam, N. (2011, June). Proximate: proximity-based secure pairing using ambient wireless signals. InProceedings of the 9th international conference on Mobile systems, applications, and services(pp. 211-224). ACM.

[25] Horn, Gnther, and Bart Preneel. "Authentication and payment in future mobile systems."Computer SecurityESORICS 98(1998): 277-293.

[26] Jaeseung Go, Kwangjo Kim. Wireless Authentication Protocol Preserving User Anonymity. SCIS 2001, Japan, January 23-26, 2001

[27] V. Miller, Use of elliptic curves in cryptography, in Proc. Adv. Cryptol. (CRYPTO85), 1985, pp. 417-426.

[28] N. Koblitz, Elliptic curve cryptosystem, Math. Comput., vol. 48, pp. 203-209, 1987.

[29] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. Springer-Verlag, 2003.

[30] Benenson, Zinaida, Nils Gedicke, and Ossi Raivio. "Realizing robust user authentication in sensor networks."Real-World Wireless Sensor Networks (REALWSN)14 (2005): 52.

[31] Jiang, Canming, Bao Li, and Haixia Xu. "An efficient scheme for user authentication in wireless sensor networks."Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on. Vol. 1. IEEE, 2007.

[32] Abi-Char, P. E., Mhamed, A., & Bachar, E. H. (2007, September). A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications. InNext Generation Mobile Applications, Services and Technologies, 2007. NGMAST'07. The 2007 International Conference on(pp. 235-240). IEEE.

[33] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, Proc. Advances in Cryptology (Crypto 84), pp. 47-53, 1984.

[34] Yang, Jen-Ho, and Chin-Chen Chang. "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem."Computers & security28.3 (2009): 138-143.

[35] Yoon, Eun-Jun, and Kee-Young Yoo. "Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ecc."Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 2. IEEE, 2009.

[36] Islam, Sk Hafizul, and G. P. Biswas. "A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem."Journal of Systems and Software84.11 (2011): 1892-1898.

[37] T. Truong, M. Tran, and A. Duong, Improvement of the more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on ECC, in Proc. 26th Int. Conf. Adv. Inf. Netw. Appl. Workshops, 2012, pp. 698-703.

[38] Debiao, He, Chen Jianhua, and Hu Jin. "An ID-based client authentication with key agreement protocol for mobile clientserver environment on ECC with provable security."Information Fusion13.3 (2012): 223-230.

[39] Wang, Ding, and Chun-guang Ma. "Cryptanalysis of a remote user authentication scheme for mobile clientserver environment based on ECC."Information Fusion14.4 (2013): 498-503.

[40] Lu, Huang, Jie Li, and Mohsen Guizani. "Secure and efficient data transmission for cluster-based wireless sensor networks." IEEE transactions on parallel and distributed systems 25.3 (2014): 750-761.

[41] Li, Jie, Huang Lu, and Mohsen Guizani. "ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs." IEEE Transactions on Parallel and Distributed Systems 26.4 (2015): 938-948.

[42] Saeed, Mutaz Elradi S., Qun-Ying Liu, GuiYun Tian, Bin Gao, and Fagen Li. "AKAIoTs: authenticated key agreement for Internet of Things." Wireless Networks: (2018) 1-21.

[43] Al-Turjman, F. and Alturjman, S., 2018. Context-Sensitive Access in Industrial Internet of Things (IIoT) Healthcare Applications. IEEE Transactions on Industrial Informatics, 14(6), pp.2736-2744.

[44] Al-Riyami, S. S., & Paterson, K. G. (2003, November). Certificateless public key cryptography. InAsiacrypt(Vol. 2894, pp. 452-473).

[45] Liu, Jingwei, et al. "Certificateless remote anonymous authentication schemes for wirelessbody area networks."IEEE Transactions on Parallel and Distributed Systems25.2 (2014): 332-342.

[46] Xiong, Hu. "Cost-effective scalable and anonymous certificateless remote authentication protocol."IEEE Transactions on Information Forensics and Security9.12 (2014): 2327-2339.

[47] Zhao, Zhenguo. "An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem." Journal of medical systems 38.2 (2014): 13.

[48] Wang, Chunzhi, and Yanmei Zhang. "New authentication scheme for wireless body area networks using the bilinear pairing."Journal of medical systems39.11 (2015): 136.

[49] He, Debiao, et al. "Anonymous authentication for wireless body area networks with provable security." IEEE Systems Journal 11.4 (2017): 2590-2601.

[50] Shen, J., Chang, S., Shen, J., Liu, Q., & Sun, X. (2016). A lightweight multi-layer authentication protocol for wireless body area networks. Future Generation Computer Systems.

[51] Li, X., Ibrahim, M. H., Kumari, S., & Kumar, R. (2017). Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors. Telecommunication Systems, 1-26.

[52] Even, S., Goldreich, O., & Micali, S. (1989, August). On-line/off-line digital signatures. In Conference on the Theory and Application of Cryptology (pp. 263-275). Springer, New York, NY.

[53] Koblitz, N. (1991, August). CM-Curves with Good Cryptographic Properties. In Crypto (Vol. 91, pp. 279-287).

[54] Certicom Corporation, Remarks on the Security of the Elliptic Curve Cryptosystem (2010) Available from http://www.secg.org/sec2-v2.pdf

[55] Oliveira, Leonardo B., et al. "Secure-TWS: Authenticating node to multi-user communication in shared sensor networks." The Computer Journal 55.4 (2012): 384-396.

[56] Aranha, Diego F., et al. "Efficient implementation of elliptic curve cryptography in wireless sensors." Adv. in Math. of Comm. 4.2 (2010): 169-187.

[57] Barreto, P. S., Kim, H. Y., Lynn, B., & Scott, M. (2002). Efficient algorithms for pairing-based cryptosystems. In Annual interna- tional cryptology conference (pp. 354-369). Berlin: Springer.

[58] Bellare, M., & Rogaway, P. (1993, December). Random oracles are practical: A paradigm for designing efficient protocols. In Proceedings of the 1st ACM conference on Computer and communications security (pp. 62-73). ACM.

[59] Certicom Corporation, Remarks on the Security of the Elliptic Curve Cryptosystem (2000). http://www.comms.engg.susx.ac.uk/fft/crypto/EccWhite3.pdf

[60] Barreto, P. S., Galbraith, S. D., higeartaigh, C., & Scott, M. (2007). Efficient pairing computation on supersingular abelian varieties. Designs, Codes and Cryptography, 42(3), 239-271.

[61] Oliveira, L. B., Aranha, D. F., Gouvła, C. P., Scott, M., Cmara, D. F., Lpez, J., & Dahab, R. (2011). TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Computer Communications, 34(3), 485-493.

[62] Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004, August). Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In CHES (Vol. 4, pp. 119-132).

[63] Crossbow, MICA2 datasheet, Available from http://www.cmt-gmbh.de/Produkte/WirelessSensorNetworks/Datenblaetter/MICA2_OEM_Edition_Datasheet.pdf

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2876133, IEEE Internet of Things Journal

[64] Shim, Kyung-Ah. "S 2 DRP: secure implementations of distributed reprogramming protocol for wireless sensor networks." Ad Hoc Networks 19 (2014): 1-8.
[65] Shim, Kyung-Ah, Young-Ran Lee, and Cheol-Min Park. "EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks." Ad Hoc Networks 11.1 (2013): 182-189.
[66] Cao, Xuefei, et al. "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks." Computer communications 31.4 (2008): 659-667.
[67] Zhang, Z., Wong, D. S., Xu, J., & Feng, D. (2006, June). Certificateless public-key signature: security model and efficient construction. In ACNS (Vol. 6, pp. 293-308).
[68] Huang, X., Mu, Y., Susilo, W., Wong, D., & Wu, W. (2007). Certificateless signature revisited. In Information Security and Privacy (pp. 308-322). Springer Berlin/Heidelberg.
[69] Choi, Kyu Young, Jong Hwan Park, and Dong Hoon Lee. "A new provably secure certificateless short signature scheme." Computers & Mathematics with Applications 61.7 (2011): 1760-1768.
[70] Saeed, M. E. S., Liu, Q., Tian, G., Gao, B., & Li, F. HOOSC: heterogeneous online/offline signcryption for the Internet of Things. Wireless Networks, (2017):1-20.
[71] Barreto, P. S., Libert, B., McCullagh, N., & Quisquater, J. J. (2005, December). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 515-532). Springer, Berlin, Heidelberg.
[72] Boneh, D., & Boyen, X. (2004, May). Short signatures without random oracles. In Eurocrypt (Vol. 3027, pp. 56-73).
[73] Pointcheval, D., & Stern, J. (2000). Security arguments for digital signatures and blind signatures. Journal of cryptology, 13(3), 361-396.
[74] Kwak, K. S., Ullah, S., & Ullah, N. (2010, November). An overview of IEEE 802.15. 6 standard. InApplied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on(pp. 1-6). IEEE.

Mutaz Elradi S. Saeed received the B.Sc. degree (Hons.) in computer science and statistics, and the M.Sc. degree in computer sciences, from Faculty of Mathematical Sciences, University of Khartoum, Khartoum, Sudan, in 2004, 2009, respectively. He also received Microsoft certificates (MCP, MCSA, MCSAM and MCSE) and Cisco certificate (CCNA) in 2006. He is a lecturer with department of computer science - Nile Valley University, he was the head of computer science department from 2012 to 2014. He is currently pursuing his Ph.D. degree in Internet of Things Security and Privacy at School of Automation Engineering, University of Electronic Science and Technology of China, China. His current research interests include Internet of Things System, Embedded System, applied cryptography, information security and security in wireless sensor networks.

Qun-Ying Liu (M13) received the B. Eng. Degree, M.S. and Ph.D. degree of electrical engineering, respectively, from Sichuan University, Chengdu, in 2000, 2005 and 2008. She is currently in School of Automation Engineering, University of Electronic Science and Technology of China, China. Her research interest is power system security and stability analysis, and advanced application of PMUs.

Gui Yun Tian (M01SM03) received the B.Sc. degree in metrology and instrumentation and the M.Sc. degree in precision engineering from the University of Sichuan, Chengdu, China, in 1985 and 1988, respectively, and the Ph.D. degree from the University of Derby, Derby, U.K., in 1998. From 2000 to 2006, he was a Lecturer, a Senior Lecturer, a Reader, a Professor, and the Head of the Group of Systems Engineering with the University of Huddersfield, U.K. Since 2007, he has been the Chair Professor of Sensor Technologies with Newcastle University, Newcastle upon Tyne, U.K. He has coordinated several research projects from the Engineering and Physical Sciences Research Council, the Royal Academy of Engineering, and FP7, and also has good collaboration with leading industrial companies, such as Airbus, Rolls Royce, BP, Network Rail, and TWI. His research interests include sensors, non-destructive test and evaluation, structural health monitoring, and Internet of Things (IOTs). He is currently an Adjunct Professor with the School of Automation Engineering, University of Electronic Science and Technology of China.

Bin Gao received the B.Eng. degree in 2005 from Southwest Jiao Tong University and M.S. and Ph.D. degree of electrical engineering, respectively, from Newcastle University, UK, in 2007, 2011. He is currently an associate professor in School of Automation Engineering, University of Electronic Science and Technology of China, China. His research interests include statistical signal processing, blind source separation, machine learning, audio and image signal processing, social signal processing and signal processing in Non-Destructive Evaluation (NDE). He is also jointly supervising PhD students from Newcastle University with Doctor W.L. Woo, Prof Guiyun Tian and Prof Dlay in the above research areas.

Fagen Li is a professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, P.R. China. He received his Ph.D. degree in Cryptography from Xidian University, Xian, P.R. China in 2007. From 2008 to 2009, he was a postdoctoral fellow in Future University-Hakodate, Hokkaido, Japan, which is supported by the Japan Society for the Promotion of Science (JSPS). He worked as a research fellow in the Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan from 2010 to 2012. His recent research interests include cryptography and network security. He has published more than 70 papers in the international journals and conferences. He is a member of the IEEE.

2327-4662 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.