Privacy Aware Incentive Mechanism to Collect Mobile Data While Preventing Duplication

Junggab Son*, Donghyun Kim*, Rasheed Hussain†, Alade Tokuta*, Sung-Sik Kwon*, and Jung-Taek Seo‡§
*Department of Mathematics and Physics, North Carolina Central University, Durham, NC, 27707
Email: {json, donghyun.kim, atokuta, skwon}@nccu.edu
†Department of Computer Science, Innopolis University, Kazan, Russia
Email: rasheed1984@gmail.com
‡The Attached Institute of ETRI, Daejeon, South Korea. Email: seojt@ensec.re.kr
§Corresponding Author.

***Abstract*—The recent technological advances in mobile devices such as smartphones foster a wide variety of emerging applications which consider users as the providers as well as consumers of the highly valuable real world data from the devices. Interestingly enough, many of the existing researches related to this topic implicitly assume that the users will actively provide mobile sensing data to enable the applications without any compensation, which is not necessarily true for many reasons, e.g. extend battery lifetime, improve system performance, etc., and thus many users are rather dormant in practice. Therefore, there is an urgent need to develop a proper incentive mechanism for the applications to transform the users to be more active so that the applications can collect much-needed high-quality data. One common key challenge to realize the incentive mechanisms is how to preserve the privacy of the users as they will be requested to provide possibly-privacy-invasive mobile data. An anonymous identity and pseudonym based scheme is a straightforward and easy-to-adopt solution to address this issue. Unfortunately, this approach makes it extremely difficult or inefficient to detect duplicated sensing data from greedy users hoping to get more incentive with the state-of-art strategies. The duplicate data can generate lots of noise when the respective application analyzes the data and will cause more cost to operate the application, and therefore is very harmful. This paper proposes a novel privacy-aware mobile incentive scheme of its kind without trusted third party (TTP) in the sense that two different messages, each of which is with the same sensing data, but with different pseudonym, from the same mobile user can be used to recover the private key of the user.**

I. Introduction

Thanks to the recent advances in sensing and mobile technologies, a number of applications which utilize the mobile data have been emerged. For instance, in vehicular ad-hoc networks (VANETs), sensors are used to measure various information from each vehicle such as acceleration, speed, global positioning coordination. At the same time, several recent research tried to use VANET nodes to collect pictures and make them to serve as witnesses of designated incidents such as accidents [8]. Additionally, a smartphone can be used to collect data from the surroundings such weather information, owners health information and so forth [4]. Such sensing data may improve the quality of application and data consumer can obtain sensing data simply through internet-based applications.

Previous research regarding sensing data show that the users are assumed to be volunteers for their applications [1]. However, users can be selfish in real world and thus are likely not to permit others to use their resources without sufficient compensation. Therefore, a service provider may not be able to obtain sufficient amount of sensing data to run their applications. Therefore, an incentive scheme is needed to motivate users and obtain better sensing data. However, sensing data contains various kinds of sensitive information that is related to users privacy such as location, health, activity, social event, billing and so on. An adversary can trace the path of a users car by analyzing traffic sensing data as well as figure out about users medical status by analyzing body sensing data used for health care. Meanwhile, the information fed to an incentive scheme may include the private information about the entities participating the scheme.

Anonymous ID and pseudonym based scheme is one of the effective solution to protect users privacy [12]. By using randomized ID instead of the actual ID, it is hard for an adversary to establish a relationship between user and sensing data. However, privacy preserving scheme can cause side effect in incentive schemes for sensing data. A dishonest user can send multiple sensing data while applying different pseudonym to earn more credit. In such scenario, it is very hard for the service provider to revoke such malicious user without revocation authority in privacy preserving system. When the service provider finds a message that contains the same data but with different pseudonyms, service provider sends it to revocation authority for checking duplication of sensing data. Then revocation authority confirms misbehavior of a user by retrieving its actual ID using the received pseudonym. This process takes a considerably long time when the system large.

In this paper, we propose a privacy preserving incentive scheme with effective checking for duplicated sensing data. We adopt the idea of secure multiple-times proxy signature scheme [2] in which the private key of the proxy signer will be revealed if the signer generates signature more than prior consultation, and a users private key will be revealed if the user sends duplicated sensing data with different pseudonyms. This approach has two advantages. First, it makes user to avoid sending multiple sensing data because the private key

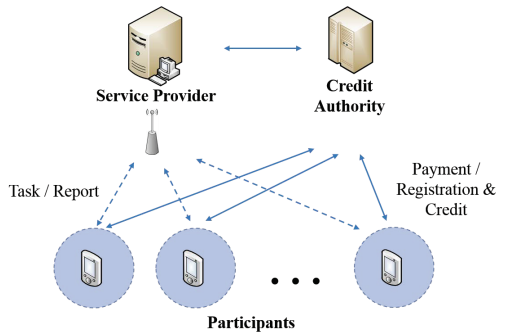

Fig. 1: System Model.

of the user will be revealed, otherwise. Second, it can revoke abnormal user efficiently. In case that a service provider finds duplicated sensing data, it can extract the secret key. Largely, the key contribution of this paper is two folds.

(a) Privacy preserving mobile incentive scheme with efficient verification of pseudonyms: In our scheme, a user can generate a pseudonym by combining service provider generated value and randomly generated value, after being registered to credit server. This means our scheme can let the user joins/leavs effectively, since it does not affect other users.

(b) Efficient and effective way to find duplicated sensing data with different pseudonyms: We design our scheme to make a user's private key revocation in case if the user sends identical sensing data with different pseudonyms. This property can prevent user's misbehavior as well as can detect duplicated sensing data efficiently. To the best of our knowledge, our scheme is the first cryptographic approach to solve duplicated data problem for privacy aware incentive scheme in mobile sensing environment.

The rest of this paper is organized as follows: we discuss background, problem statement, and some preliminaries described in Section II. Our proposed scheme is introduced in Section III, and analysis of the proposed scheme is represented in Section IV. Finally, we conclude the paper in Section V.

II. Background, Problem Statement, and Preliminaries

A. System Model

Fig. 1 illustrates the system model for privacy-aware mobile incentive mechanism. We define three different entities and they can be identified as follows.

- **Service provider (SP):** It receives sensing tasks from DC, distributes them to the participants in the vicinity of the site of interest. SP also analyzes and processes sensing data to make it available to the data consumer. After sensing task is completed, SP sends credit as reward for a task to the participants.
- **Credit authority (CA):** A participant has to register with the CA before performing a sensing task. When a participant sends credit that is received from SP, CA stores it with credit ID (CID) of the participant. We treat CA as semi-trusted entity that has the role of user and credit management. The term semi-trusted means that CA manages users personal information securely, not in the control of whole system.
  The CA is needed only for payment reason, thus virtual money system such as bitcoin can be applied to preserve privacy while using and rewording a credit.
- **Participants:** It reports sensing data collected by sensors in mobile nodes to an SP, and earns credit from the SP. A participant has to register with CA for processing sensing tasks, and deposit credits. We will use participants and users interchangeably in the following descriptions.

We use the SP and the CA separately for the distribution of authority. In the real application, a CA and SP are completely different entities. For instance, a bank or a credit card company have role of the CA and any kind of service provider such as an auction provider, a network provider have role of SP. A SP never makes payment process with user directly, but through payment system of a CA. Similar like this, our system uses CA to process credit.

B. Problem Definition

From a given set of sensing report for a sensing request $\mathcal{R} = \{\nabla_{p_1}, \nabla_{p_2}, \ldots, \nabla_{p_j}\}$, where p_j is pseudonym which contained in sensing report, find two or more same sensing reports that made from a user.

A sensing report collected by users mobile device may has privacy related data depending on consuming applications. A sensing report for the health monitoring application contains users body conditions such as electrocardiogram. A sensing report for the VANET application contains driving information such as visiting location and GPS information. In addition, the incentive scheme also contains various sensitive information in which who performed sensing tasks, how many tasks a user performed, and so on. Therefore, privacy preserving scheme is a necessity for incentive scheme in mobile sensing environment.

Although privacy preserving scheme is important, it causes side effect: possibility of sensing report duplication attack. Assume that a SP applied anonymous ID scheme to protect user privacy. In this case, each user has multiple pseudonym and it is used as anonymous ID. When a user completed a sensing task, the user generates many sensing report just applying different pseudonym on it. In case if sensing report has simple general information, which temperature, GPS, and density of human or cars in specific area, it is hard to distinguish that comes from same user or not. An attacker can make unfair profits from sensing report duplication attack. Therefore, an effective scheme to detect duplicated sensing report is needed.

C. Adversary Model

We consider the adversary model in terms of incentive and privacy.

- **Attacks on Incentive**: A user participating in mobile sensing system may try to earn more credit than expected for sensing task. One possible attack is making a lot of reports with same sensing data and each report consists of different pseudonyms. We call this attack as "sensing data duplication attack" and multiple sensing reports consist of same sensing result and different pseudonym as "duplicated sensing data". On the other hand, SP may try to pay less credit than assigned credit on sensing task or a malicious SP may even skip to pay the credit.
- **Attacks on Privacy**: During sensing and reporting for a task, a users privacy can be evaded by SP or other attacker. They can collect sensing data from specific user and obtain sensitive users data such as performed tasks, location and credit information and others. A malicious SP can easily identify a user through announcing a task which targets a narrow set of users. This problem is not unique to our scenario, and it can be solved by task verification scheme which is only verified task can be published by SP [12]. Since this solution can be easily applied to our proposed scheme, we omit it from this paper.

D. Design Goals

We design our privacy aware incentive mechanism with preventing duplicated sensing data under the following requirements.

- **User privacy:** Incentive schemes in mobile sensing need to preserve user privacy. Attacker who eavesdrops a sensing data during transmission or service provider who collects sensing data from user cannot know that a sensing data was sent from a particular user. Also, attacker cannot know if the given set of sensing data was sent by the same user.
- **Detecting duplicated sensing data:** If a user sends the same sensing data with different pseudonyms to earn more credit, SP has to detect users misbehavior. In this case, SP can send request for revocation to the CA.
- **Protecting credit:** A credit is valid only for given pseudonym, and once a credit issued, it cannot be revoked unilaterally by SP. A credit can never be used more than twice.

E. Assumptions

In this paper, we establish following two assumptions.

- We assume that the CA, SP and each user have a public/private key pair, which can be used to authenticate each other and digital signature. These keys and certificates are issued by a certified authority.
- We assume that the communications between users and the SP are anonymized (e,g., with IP and MAC address recycling techniques or Mix Networks [12]).

F. Preliminaries

The notation used in this paper are listed in Table 1. Next, we introduce three important definitions.

TABLE I: Notations.

Notation	Description
q	k-bit prime number
$\mathbb{Z}_q$	Integers modulo q
$\mathbb{G}, \mathbb{G}_T$	Cyclic group with prime order q
g	Generator of $\mathbb{G}$
e	Bilinear pairing that satisfies with $\mathbb{G} \times \mathbb{G}_T$
U_i	User i
pk_i, sk_i	Public/private key pair of U_i
pk_c, sk_c	Public/private key pair of CA
pk_s, sk_s	Public/private key pair of SP
m	Sensing Data, $m = \{0,1\}^n$
$H()$	$\{0,1\}^* \rightarrow \mathbb{Z}_q$
T	Token issued by CA
p_j	A pseudonym generated by a user
$\mathcal{R}_{p_j}$	Sensing report with pseudonym p_j
$\mathcal{C}_j$	Credit for pseudonym p_j
ss_i	session secret for credit reward

Definition 1 (DDHP)**.** *The decisional diffie-dellman problem (DDHP) [16] states that, given g^a and g^b for uniformly and independently chosen $a, b \in \mathbb{Z}_q$, the value g^{ab} looks like a random element in $\mathbb{G}$.*

This intuitive notion is formally stated by saying that the following two probability distributions are computationally indistinguishable (in the security parameter, $n = log(q)$):

(a) (g^a, g^b, g^{ab}), where a and b are randomly and independently chosen from $\mathbb{Z}_q$.

(b) (g^a, g^b, g^c), where a, b, c are randomly and independently chosen from $\mathbb{Z}_q$.

Definition 2 (Bilinear map)**.** *A bilinear map is a map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties [17], [18].*

(a) Computable: there exists an efficiently computable algorithm for computing e,

(b) Bilinear: for all $h_1, h_2 \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p, e(h_1^a, h_2^b) = e(h_1, h_2)^{ab}$, and

(c) Nondegenerate: $e(g, g) \neq 1$, where g is a generator of $\mathbb{G}$.

Definition 3 (DBDH)**.** *The decisional bilinear diffie-hellman (DBDH) problem in groups $(\mathbb{G}, \mathbb{G}_T)$ is, given a tuple $(g, g^a, g^b, g^c, Z) \in \mathbb{G}^4 \times \mathbb{G}_T$ with unknown $a, b, c \in_R \mathbb{Z}_q$, whether $Z = e(g, g)^{abc}$. A polynomial-time algorithm $\mathcal{B}$ has advantage ϵ in solving the DBDH problem in groups $(\mathbb{G}, \mathbb{G}_T)$, if*

$$|(Pr[(g, g^a, g^b, g^c, \mathbb{Z} = e(g, g)^{abc}) = 1] - Pr[(g, g^a, g^b, b^c, \mathbb{Z} = e(g, g)^d) = 1])| \geq \epsilon,$$

where the probability is taken over the random choices of $a, b, c, d \in \mathbb{Z}_q$, the random choice of g in $\mathbb{G}$, and random bits consumed by $\mathcal{B}$.

III. Proposed Scheme

We aim to design privacy aware mobile incentive scheme with detecting duplicated sensing data. To the best of our knowledge, our scheme is the first cryptographic approach to solve duplicated data problem for privacy aware incentive scheme in mobile sensing environment.

The proposed scheme makes a group with users who perform the same task and finds duplicated sensing data by

the group for efficiency. We design pseudonym based privacy preserving scheme which is verifiable and revokable. In our scheme, a user can generate a valid pseudonym without the help of certificated authority. And our scheme can reveal illegal users private key by applying idea of multiple times proxy signature schemes [2].

This approach can avoid users misbehavior by revealing private key which is much more critical than earning credit from such misbehavior. In addition, private key in a pseudonym will be cancelled out (not revealment) if a user sends same sensing data with same pseudonym. This case can be made by network problem and our scheme still working.

A. Setup

On inputing a security parameter 1^k, the setup process first determines $(q, \mathbb{G}, \mathbb{G}_T, e)$. Next, it chooses $g \in_R \mathbb{G}$, and three hash functions $H_1() : \{0,1\}^* \rightarrow \mathbb{Z}_q, H_2() : \{0,1\}^* \rightarrow \{0,1\}^n, H_3() : \mathbb{G} \rightarrow \{0,1\}^*$. The global parameters are

$$((q, \mathbb{G}, \mathbb{G}_T, e), H_1(), H_2(), H_3()).$$

The client generates a public/private key pair (pk_i, sk_i). The client picks $sk_i \in_R \mathbb{Z}_q$, and computes g^{sk_i}. The private key is sk_i and the public key is $pk_i = g^{sk_i}$. Same as U_i, a SP and CA also generates a public/private key pair $(pk_s, sk_s), (pk_c, sk_c)$, respectively.

B. Registration and pseudonym generation

To perform and earn credit using sensing data, a user has to register to the CA. We use Account ID (AID) as identification factor. It uses only for saving and reward credit like a bank account or a credit card number. For the privacy reason, a users AID can be changed periodically. However, a credit cannot move from one AID to another AID for revocation reason. Since users credit is stored at the CA, an attacker can get reward from CA even after revoked from SP. To prevent this problem, we make link between AID and sk_i to revoke not only public/private key pair but also AID in case of users misbehavior.

To make account on the CA, U_i generates a set of pseudonyms first. A pseudonym consists of user's secret key and uses (t, n) secret sharing scheme to recover the secret key in case of sensing data duplication attack. A pseudonym generation process is as follows:

1) Picks X, r randomly
2) Splits X into n numbers using $(2, n)$-secret sharing scheme [19], $\mathcal{X}_s = \{x_0, x_1, x_2, \ldots, x_n\}$. This means any two or more x can rebuild X by combining using secret sharing computation: $\exists \partial$ in $\mathcal{X}_s, X = \sum_{\ell=1}^{2 \le \ell \le n} \partial_\ell$
3) Computes $x'_k = \{x_k / X\}_{0 \le k \le n}$
4) Computes a set of pseudonyms $\mathcal{P} = \{p_k\}_{1 \le k \le n}, p_k = sk_i^{x'_k} \cdot r \in \mathbb{Z}_q$
5) Makes pseudonym verification value $\mathcal{V}$: $\mathcal{V} = \{v_1, v_2\}, v_1 = g^r, v_2 = sk_i^{x'_0}$

After generating a set of pseudonyms, U_i sends $\mathcal{P}, AID, \mathcal{V}$ to the CA. The CA verifies a set of pseudonym by computing follow equations:

$$\begin{aligned} e(v_1^n, pk_i) &\stackrel{?}{=} e(g, g^{\prod_{k=1}^n p_k}) \\ &= e(g, g^{r \cdot n \cdot sk_i^{\sum_{k=1}^n x'_k}}) \\ &= e(g, g)^{r \cdot n \cdot sk_i}, \end{aligned} \tag{1}$$

where p_k is randomly selected pseudonym from $\mathcal{P}, p_k \in_R \mathcal{P}$. The CA can verify all of pseudonyms at once through (1), also can verify a pseudonym one by one using v_2:

$$e(v_1, pk_i) \stackrel{?}{=} e(g, g^{v2 \cdot p_k}). \tag{2}$$

If true, the CA makes verification factor $(V)'$ for a set of pseudonyms:

$$\begin{aligned} \mathcal{V}' &= (v'_1, v'_2), \\ v'_1 &= pk_i^{sk_c}, \\ v'_2 &= (g^{v_2})^{sk_c}. \end{aligned} \tag{3}$$

The CA stores $\{AID, (V)', \mathcal{P}\}$, and sends $(V)'$ to the U_i. The U_i can verify $(V)'$ as follows:

$$v'_1 \stackrel{?}{=} pk_c^{sk_i}, v'_2 \stackrel{?}{=} pk_c^{p'_0}. \tag{4}$$

If true, U_i uses $\mathcal{P}$ as valid pseudonym. After certain period of time, a user may want to replace pseudonym for the privacy reason. In this case, a user generates new pseudonym using the (1)$\sim$(4) equations.

C. Sensing Request and Report

To announce a sensing task, the SP assigns unique task number T_{ID} on a requirement. The SP generates random number $k \in_R \mathbb{Z}_q$ and computes ρ for a sensing task:

$$\rho = H_1(T_{ID}) sk_s + kK,$$

where $K = g^k$. SP stores T_{ID}, ρ, k and sends T_{ID}, ρ, K to users. After receiving it, the U_i verify validation as follow:

$$g^\rho \stackrel{?}{=} pk_s^\epsilon \cdot K^K \in \mathbb{G},$$

where $\epsilon = H_1(T_{ID})$. If $true$, the U_i performs the sensing task.

After completed a sensing task, U_i picks a pseudonym randomly from $\overline{\mathcal{P}}, p_k \in_R \mathcal{P}$ and picks $\tau, s \in_R \mathbb{Z}_q$, then generates sensing report $\mathcal{R}$ as follows:

$$\begin{aligned} \mathcal{R}_{p_k} &= (\gamma_1, \gamma_2, \gamma_3, \gamma_4), \\ \gamma_1 &= \overline{p_k}^{H_1(T_{ID})} \\ \gamma_2 &= m \oplus H_2(T_{ID} || H_3(pk_s^\tau)), \\ \gamma_3 &= g^\tau, \gamma_4 = g^s. \end{aligned}$$

The U_i sends $T_{ID}, \mathcal{V}', \mathcal{R}_{p_k}$ to the SP as report of the sensing request. Then, the SP checks validity of $\mathcal{R}_{p_k}$ as follows:

$$\begin{aligned} e(pk_c^{H_1(m)}, v_1') &\stackrel{?}{=} e(g^{\gamma_1}, v_2') \\ &= e(g^{sk_i^{p_k'} \cdot H_1(m)}, g^{sk_i^{p_0'} \cdot sk_c}) \\ &= e(g,g)^{H_1(m) \cdot sk_c \cdot sk_i} \end{aligned}$$

If true, the SP decrypts sensing data as follows:

$$m = \gamma_2 \oplus H_2(T_{ID} || H_3(\gamma_3^{sk_s})).$$

D. Receiving and saving Credit

After accepting the sensing data, the SP has to issue credit ω with credit ID (CID) for U_i. The SP generates valid ω and verification messages for received pseudonym of sensing report as follows:

$$\begin{aligned} \mathcal{C} &= \{c_1, c_2, c_3, c_4\}, \\ c_1 &= CID, \\ c_2 &= \omega \oplus H_2(CID || H_3(\gamma_4^{sk_s})), \\ c_3 &= \gamma_4^{sk_s \cdot H_1(p_k) \cdot H_1(\omega) \cdot H_1(CID)}, \\ c_4 &= v_1'^{sk_s \cdot H_1(p_k) \cdot H_1(\omega) \cdot H_1(CID)}. \end{aligned}$$

The SP sends $\mathcal{C}$ to the U_i. The U_i decrypts ω from c_2:

$$\omega = c_2 \oplus H_2(CID || H_3(pk_s^s)).$$

Then the U_i checks its validity as follows:

$$c_3 \stackrel{?}{=} pk_s^{s \cdot H_1(p_k) \cdot H_1(\omega) \cdot H_1(CID)}$$

If true, the U_i stores $\mathcal{C}$ computes $\mathcal{C}'$:

$$\begin{aligned} \mathcal{C}' &= \{c_1', c_2', c_3', c_4'\}, \\ c_1' &= CID, \\ c_2' &= \omega \oplus H_2(CID || H_3(pk_s^s)), \\ c_3' &= g^s, c_4' = c_4 \end{aligned}$$

The U_i sends $AID, p_k, \mathcal{C}'$ to the CA. First, the CA checks p_k is allocated to AID. If true, the CA decrypts ω from c_2':

$$\omega = c_2' \oplus H_2(CID || H_3(c_3'^{sk_c})).$$

Then, the CA checks its validity as follows:

$$\begin{aligned} e(g, c_4') &\stackrel{?}{=} e(pk_i^{H_1(p_k)}, pk_s^{H_1(\omega) \cdot H_1(CID)} \\ &= e(g,g)^{sk_i \cdot sk_s \cdot H_1(p_k) \cdot H_1(\omega) \cdot H_1(CID)} \end{aligned}$$

If true, the credit is valid and the CA accepts it.

E. Revealing user's private key

In case if U_i sends same sensing data with different pseudonyms more than once, the private key of U_i will be revealed as follows:

1) From two sensing data $\mathcal{R}_{p_\alpha}, \mathcal{R}_{p_\beta}$, where $1 \leq \alpha, \beta \leq n$
2) Computes $p_\alpha \cdot p_\beta$:

$$\begin{aligned} & sk_i^{H_1(m) \cdot p_\alpha / X} \cdot sk_i^{H_1(m) \cdot p_\beta / X} \\ = \; & sk_i^{H_1(m) \cdot (p_\alpha + p_\beta)} = sk_i^{H_1(m)} \end{aligned}$$

3) Recover sk_i by computing $(sk_i^{H_1(m)})^{-H_1(m)}$, where $-H_1(m)$ is multiplicative inverse of $H_1(m) \in \mathbb{Z}_q$. It is easily computed using the extended Euclidean algorithm.

IV. Analysis

This section analyzes security and efficiency of the proposed scheme. The main purpose of the proposed scheme is to provide privacy preserving incentive scheme with detecting duplicated messages for mobile sensing system. Therefore, we need to prove that the proposed scheme can securely provide incentives based on pseudonym.

A. Privacy Preservation

There are three points where the privacy of a user can be invaded: registration, reporting sensed data, receiving credit. In registration process, a user sends token received from CA, and it contains private key of the user. However, it is hard to find a relationship between g^{sk_i} which is private key of the user and $g^{n \cdot sk_i}$ which is the part of token made by CA. Also, for an SP is hard to find a relationship from $g^{n_1 \cdot sk_i}, g^{n_2 \cdot sk_i}, \ldots, g^{n_m \cdot sk_i}$ under the DDHP.

A pseudonym which is used to report sensed data and receive credit has randomized value r_j. Since a token can pass the verification process without public key of a user in registration step, an SP has a negligible probability to find relationship from $p_1, p_2, \ldots, p_j$. Additionally, an SP cannot link a credit token with another one and a credit token with a user, since pseudonym has been anonymized using the randomized value, and pseudonym is only for one time use. Therefore, pseudonym and credit does not help an SP to break a users privacy.

B. Security on Incentives

Without loss of generality, let us consider the following three attack models from users point of view. First, a dishonest user may sends multiple sensing data to an SP. In this case, the private key of the user will be revealed, which is one of our contributions. This property can make user to avoid sending duplicated data as well as SP to revoke user without cooperation of TTP. Second, a dishonest user may eavesdrop other credit and sends it to CA as its own credit. In this case, the dishonest user cannot pass the verification process of CA, and it can be revoked. Third, a dishonest user may sends same credit to the CA repeatedly to earn more credit. Since the credit has task number and it stores on actual ID, it can be detected easily by CA.

From an SP's standpoint, we can consider that the SP sends less or no credit for a task. Since we apply digital signature scheme on the credit token, and the security of credit toke is based on the security of applied digital signature scheme.

C. Efficiency

Our proposed scheme is the first approach to detect duplicated sensing data in privacy aware mobile incentive scheme. Therefore, compared with general pseudonym revocation

scheme, we analyze efficiency of the proposed scheme in point of detecting a misbehaving user.

In case of general pseudonym revocation, a system needs revocation authority. The term revocation authority (RA) means that it has ability to revoke user. It knows the relationship between actual ID and pseudonym. For this reason, an SP cannot be a RA. The RA has the role of authentication of user and stores a set of pseudonym for each user.

When an SP finds a set of sensing data which is expected to be duplicated, SP sends it to RA. Then, RA retrieves actual ID with a set of pseudonym using one of the received pseudonym, and checks another pseudonym belonging to that pseudonym set. Suppose that there are u users in a sensing application and each user has p pseudonyms. In case of the SP sends l of pseudonyms as suspect, the total computational cost to find misbehavior user is $\frac{u(p \times l)}{2}$.

In our proposed scheme, duplicated message leaks a private key of a misbehavior user. Since it is very critical disadvantage to the user, this property makes user to avoid sending duplicated sensing data. However, in case of an SP need to revoke dishonest user, it computes suspect private key from sensing data first. Then, the SP can find the owner of private key easily or applies to CA to revoke the user. In case if SP sends suspect private key to CA, same as request to RA of our first consideration, the CA needs to check only u times to find actual ID. Therefore, our scheme can reduce cost to find actual ID from the huge pseudonym forest.

V. Conclusion

In privacy-aware incentive scheme in mobile sensing, it is hard to detect duplicated sensing data with different pseudonyms. To address this problem, we designed our scheme in which the service provider can revoke the private key of a user who sends duplicated sensing data. To the best of our knowledge, our scheme is the first cryptographic approach to solve duplicated data problem of privacy aware incentive scheme in mobile sensing environment. This mechanism makes user to avoid sending duplicated sensing data as well as it can detect duplicated sensing data without trusted entity.

Acknowledgment

This work was supported in part by US National Science Foundation (NSF) CREST No. HRD-1345219 and HRD-1533653. This research was also supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support programs (IITP-2015-H8501-15-1007, IITP-2015-H8501-15-1018) supervised by the IITP (Institute for Information & communications Technology Promotion). This work was also supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2012R1A2A2A01046986).

References

[1] E. Miluzzo, N. Lane, K. Fodor, R. Peterson, H. Lu, M. Musolesi, S. Eisenman, X. Zheng, and A. Compbell, "Sensing Meets Mobile Social Networks: the Design, Implementation and Evaluation of the CenceMe Application," in *Proceedings of the 6th International Conference on Embedded Networked Sensor Systems*, pp. 138-155, Nov. 2008.

[2] X. Hong and K. Chen, "Secure multiple-times proxy signature scheme," *Computer Standards&Interfaces*, vol. 31, pp. 19-23, Jan. 2009.

[3] X. Sheng, J. Tang, X. Xiao, and G. Xue, "Sensing as a Service: Challenges, Solutions and Future Directions," *IEEE Sensors journal*, vol. 13, no. 10, pp. 3733-3741, Oct. 2013.

[4] M. Mun, "PEIR, the Personal Environmental Impact Report, as a Platform for Participatory Sensing Systems Research," in *Proceedings of the 7th international conference on Mobile systems, applications, and services*, pp. 55-68, June 2009.

[5] S. Consolvo, "Activity Sensing in the Wild: A Field Trial of Ubifit Garden," in *Proceedings of the 6th international conference on Mobile systems, applications, and services*, pp. 1797-1806, Apr.2008.

[6] P. Mohan, V.N. Padmanabhan, and R. Ramjee, "Nericell: Rich Monitoring of Road and Traffic Conditions using Mobile Smartphones," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*, pp. 323-336, Nov. 2008.

[7] A. Thiagarajan, "VTrack: Accurate, Energy-Aware Road Traffic Delay Estimation using Mobile Phones," in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, pp. 85-98, May 2009.

[8] J. Lee and B. Hoh, "Sell Your Experiences: A Market Mechanism based Incentive for Participatory Sensing," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications*, pp. 60-68, Apr. 2010.

[9] L. Duan, "Incentive Mechanisms for Smartphone Collaboration in Data Acquisition and Distributed Computing," in *Proceedings of the IEEE INFOCOM*, pp. 25-30, Mar. 2012.

[10] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to Smartphones: Incentive Mechanism Design for Mobile Phone Sensing," in *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking*, pp. 173-184, Dec. 2012.

[11] B. Di, T. Wang, L. Song, and Z. Han, "Incentive Mechanism for Collaborative Smartphone Sensing using Overlapping Coalition Formation Games," in *Proceedings of the IEEE Globe Communication Conference*, pp. 1705-1710, Dec. 2013.

[12] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "AnonySense: Privacy-Aware People-Centric Sensing," in *Proceedings of the 6th international conference on Mobile systems, applications, and services*, pp. 211-224, Jun. 2008.

[13] Q. Li, G. Cao, and T. La Porta, "Efficiency and Privacy-Aware Data Aggregation in Mobile Sensing," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 2, pp. 115-129, Mar. 2014.

[14] X. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Enabling Reputation and Trust in Privacy-Preserving Mobile Sensing," *to appear in a future issue of IEEE Transactions on Mobile Computing*.

[15] Q. Li and G. Cao, "Providing Privacy-Aware Incentives for Mobile Sensing," in *Proceedings of IEEE International Conference on Pervasive Computing and Communications*, pp. 76-84, Mar. 2013.

[16] D. Boneh, "The Decision Diffie-Hellman Problem," in *Proceedings of the 3rd Algorithmic Number Theory Symposium. Lecture Notes in Computer Science*, vol. 1423, pp. 48-63, 1998.

[17] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," in *Proceedings of the 7th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT)*, pp. 514-532, 2001.

[18] Hazewinkel, Michiel, "Bilinear Mapping," *Encyclopedia of Mathematics, Springer*, 2001.

[19] C.C. Yang, T.Y. Chang, M.S. Hwang, "A (t, n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, issue. 2, pp. 483-490, Apr. 2004.