Mathematical and Computer Modelling 55 (2012) 45–57

Contents lists available at SciVerse ScienceDirect

Mathematical and Computer Modelling

journal homepage: www.elsevier.com/locate/mcm

A scalable and privacy-preserving child-care and safety service in a ubiquitous computing environment

Jangseong Kim [a], Kwangjo Kim [a], Jonghyuk Park [b], Taeshik Shon [c,*]

[a] Department of Information and Communications Engineering, KAIST, Daejeon 305-714, Republic of Korea

[b] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 139-743, Republic of Korea

[c] Division of Information and Computer Engineering, College of Information Technology, Ajou University, Suwon 443-749, Republic of Korea

ARTICLE INFO

Article history:
Received 27 September 2010
Accepted 5 January 2011

Keywords:
Child-care service
Sensor network
Ubiquitous IT city
Privacy protection

ABSTRACT

Recently, the technologies for child care and safety have been developing rapidly, together with the various IT convergence services. In particular, several mobile operators (e.g., SKT, KTF, and LGT) in Korea and Gangnam province in Seoul provide their own child-care services. However, some problems such as incorrect location information, privacy violation, and difficulty of an end-user to control the child-care service still exist.

In this paper, we derive the security requirements of a child-care and safety service and establish a conceptual model satisfying the requirements. Based on the system model, we propose a privacy-preserving location supporting protocol for a child-care and safety service using wireless sensor networks. While addressing the above problems, our protocol can be operated over various networks (e.g., Wi-Fi and UWB) providing an RSSI (received signal strength indication) without any modification. Through performance and security analysis of our protocol, we show that our protocol is efficient and secure. More precisely, our protocol reduces the computation and communication overhead of the existing infrastructures to support better scalability.

1. Introduction

Recently, ubiquitous technologies such as RFID and sensor networks have become a part of our daily life. A typical example is the ubiquitous IT city called the u-City, which promises to provide better quality of life for an inhabitant of the city, raise competitiveness of a company, and support effective management through various services (e.g., ubiquitous port, ubiquitous health care, ubiquitous office, and ubiquitous safety). Several cities such as Hong Kong [1], Seoul [2], and Osaka [3] have a plan to introduce these technologies into our lives.

Compared to 10 years ago, 61.4% people in Korea feel that the safety level has changed to unsafe, as shown in Fig. 1. Also, as heinous crimes against children increase, many parents worry about their children's safety during commuting to a school or playground near their home. Moreover, 54.1% people expect that the safety level of our society will deteriorate in the near future. Therefore, u-City could be one of the promising technologies to provide child-care service to its inhabitants. To address this situation, current approaches by mobile service providers and local provinces in Korea suggest a service providing periodic reports of a child's location to his/her parents. Mobile service providers such as SKT, KTF, and LGT provide their own child-care and safety service, and the numbers of subscribers to these services are continuously increasing. In addition, Gangnam province in Seoul has provided 'u-safe Gangnam', a child-care and safety service, for its inhabitants, including disabled persons, and elderly persons who live alone, from May 2009 [4].

* Corresponding author.
E-mail addresses: taeshik.shon@gmail.com, tsshon@ajou.ac.kr (T. Shon).

0895-7177/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.mcm.2011.01.012

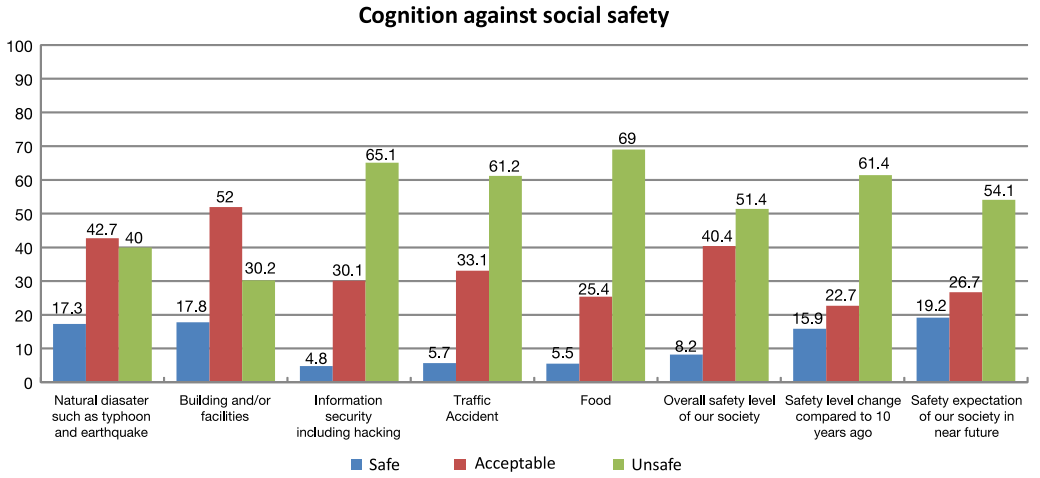

Fig. 1. Cognition against social safety [9] in Korea.

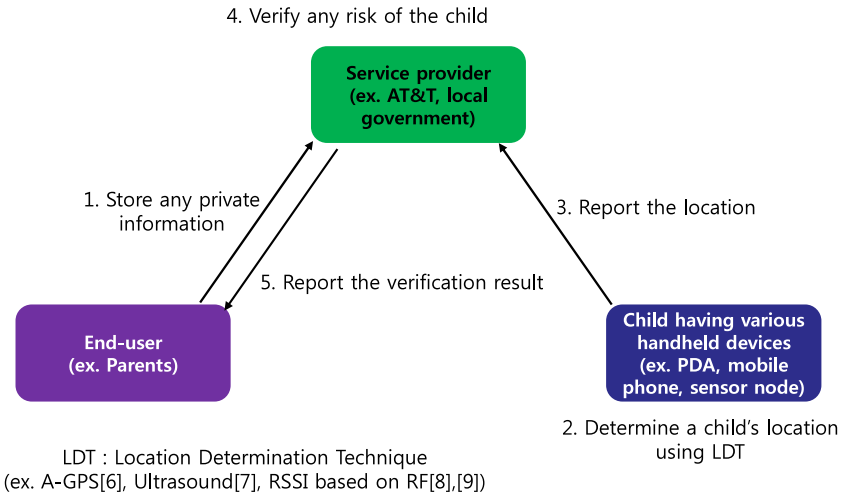

Fig. 2. Existing model for a child-care and safety service.

From now on, we call this service a child-care and safety service. Then, we can define the service using three components: the end-user, the service provider, and the device. The end-user requests the service provider to send the location information of his/her child having a proper device where the location is determined by various techniques such as A-GPS [5], ultrasound [6] and RSSI based on RF [7,8]. Fig. 2 illustrates the detailed activities among an end-user, service provider, and child. When the end-user becomes a legitimate subscriber to a child-care and safety service, the user should store the private information (e.g., his/her mobile phone number, home address, frequent visiting place, etc.) to the service provider. Then, a child who has the proper device can report his/her location to the end-user through the service provider. Using the received location information, the service provider analyzes the risk of the child. If any emergency situation has occurred or periodic reporting is required, the service provider sends the analyzed result to the end-user.

However, the existing approaches have several problems: the location information is incorrectly provided due to the number of deployed stations and technology limitation; the privacy of an end-user can be violated by private information being stored in a server of service provider; and an end-user cannot control these services. At this point, these services cannot satisfy the security requirements of the residents of the u-City.

Our contribution: In this paper, we propose a privacy-preserving child-care and safety service using the sensor network deployed in u-City. Although we employ triangulation based on RSSI [7] from three or more legitimate sensor nodes to the specific technique of our location determination, various techniques such as RSSI of Wi-Fi and UWB can be applied to our protocol without any modification if the device of the target child supports the techniques. The end-user can preserve his/her private information by restricting the role of the child-care and safety service provider to issue an authorized credential for an end-user's anonymity. The end-user can register and deregister the service, allowing choice over when to use the service. In previous approaches, an end-user could not deregister the service until the user is a legitimate subscriber of the child-care and safety service.

Our protocol delegates the role of location determination to a child's device so that the deployed sensor nodes do not require authenticating the child's device for location determination. Through reducing the energy consumption of the deployed nodes due to communication cost, our protocol can support better scalability. In addition, we show the efficiency of our protocol by illustrating the storage, computation and communication cost. More precisely, our protocol satisfies lightweightness as the child's device only requires symmetric key operations and hash operations. Finally, our approach needs less deployment cost by maximizing usage of the deployed sensor network.

Organization: The organization of this paper is as follows. In Section 2, we discuss related work and the security requirements for a child-care and safety service; then, we present our protocol for a child-care and safety service in Section 3, and provide a performance and security analysis in Section 4; finally, we conclude this paper with short summary in Section 5.

2. Background

2.1. Security requirements for a child-care and safety service

A child-care and safety service in u-City should satisfy the following security requirements.

Mutual authentication: Mutual authentication is required since each end-user and service provider want to identify whether the communicating party is a legitimate entity or not. When mutual authentication is not provided, an adversary can impersonate a specific end-user or service provider.

Privacy protection of an end-user: On the one hand, mutual authentication provides one functionality that an end-user and service provider identify each other; on the other hand, it enables an adversary to track the end-user. Also, current child-care and safety services enforce an end-user to store private information on a server of the service provider. As a result, a malicious administrator of the service provider may expose the stored private information to an adversary. Moreover, the end-user cannot control the child-care and safety service if he/she does not want to observe the child's location during some time period. This situation helps an adversary to track the end-user because a malicious administrator at the service provider can expose the child's location to the adversary. Hence, the privacy of the end-users should be protected.

Confidentiality and integrity: The location information should be encrypted with a shared key, only known to the child's parents, so that the location information is only known to the child's parents. Also, location information can be modified unless the child-care and safety service does not support integrity. Thus, confidentiality and integrity should be provided.

Scalability: The child-care and safety service should support the number of inhabitants having several devices in u-City by minimizing the effect of device addition.

Lightweightness: As one of the main characteristics in u-City is heterogeneous, the cryptographic protocols running on several devices should be lightweight with respect to communication and computation cost.

Heterogeneous network: In u-City, various networks such as 3GPP, Wi-Fi, and sensor networks may coexist. While an end-user is accessing the various networks in order to support his/her mobility, the privacy of the end-user should be protected.

2.2. Related work

2.2.1. Child-care and safety service

In Korea, mobile service providers (e.g., SKT, KTF, and LGT) provide a child-care and safety service. The service providers send the child's location information to the parent's mobile phone per every hour and send an alarm message if the child is out of his/her safety zone, predetermined by the parent. However, this approach has the following disadvantages: the child's location is not precise, due to the inaccuracies in A-GPS (network-assisted global positioning system) [5], the typical method of location determination technology; private information such as safety zone and mobile phone needs to be stored in the server of the mobile operator; an end-user cannot control the child-care and safety service if he/she does not want to observe the child's location during some time period. Gangnam province in Seoul also provides a similar service to an end-user.

In the open literature, Takata et al. [10] have proposed a dangerous location aware system for assisting child safety. They assume that each child has a proper mobile device communicating with a server in his/her home and that a public alerting service identifying several dangerous locations with real-time traffic exists. Compared to the commercial services, the system can preserve the privacy of an end-user by storing any private information in his/her home server and determining the child's location in the child's device. However, direct communication between the child's device and the home server is expensive and impractical since the devices should support various networking technologies according to the nearby environment. From this, we believe that their approach is not proper in u-City.

2.2.2. Analytical model for a sensor network

In 2004, Polastre et al. [11] proposed an analytical model for a real-world monitoring application to present the efficiency of their medium access control protocol and validated the analytical model by performing several micro benchmarks. In addition, as the analytical model is independent of the medium access control, the model is useful for analyzing the operation of a wireless sensor network application. To illustrate a sensor node's lifetime, the model in [11] computes the overall energy

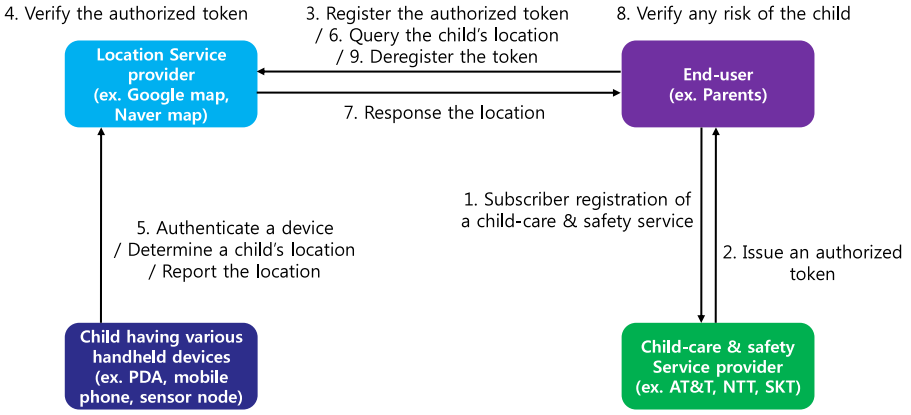

Fig. 3. Our abstract model for a child-care and safety service.

consumption of the target sensor node as follows: $E = E_{rx} + E_{tx} + E_{\text{listen}} + E_d + E_{\text{sleep}}$, where E_{rx}, E_{tx}, E_{listen}, E_d, and E_{sleep} are the energy consumption caused by receiving a message, sending a message, listening to a message, sampling data, and sleeping.

Note that E_{listen} and E_{sleep} are determined by the medium access control protocol. Also, E_d is related to the purpose of the target application and is not required for the child's safety care service. Hence, we only focus on E_{rx} and E_{tx}. The energy consumed by transmitting, E_{tx}, is $r \times |m| \times t_{txb} \times c_{txb} \times V$, where r is the message transmission rate, $|m|$ is the length of the message m, t_{txb} is the time for transmitting 1 byte, c_{txb} is the current consumption for transmitting 1 byte, and V is the voltage.

Also, the energy consumed by receiving, E_{rx}, is $z \times r \times |m| \times t_{rxb} \times c_{rxb} \times V$, where z is the number of received messages from its neighbors, t_{rxb} is the time for receiving 1 byte, and c_{rxb} is the current consumption for receiving 1 byte.

Note that when we use a Mica2 mote having a CC1000 transceiver as the sensor node, t_{txb}, c_{txb}, t_{rxb}, c_{rxb}, voltage, and capacity of battery are 416 ms, 20 mA, 416 ms, 15 mA, 3 V, and 2500 mAh.

3. Our system and protocol

In this section, we describe our system and the protocol for the child-care and safety service in detail.

3.1. Our conceptual model

To satisfy these security requirements, we propose the following conceptual model based on four components: end-user (e.g., a parent of the child), location information provider, service provider, and device. When the end-user becomes a legitimate subscribers of the child-care and safety service provider, the he/she obtains an authorized credential for the service from the service provider. Whenever the end-user wants to receive location information of his/her child, he/she should register the service with the location information provider and request a periodical location report of the child. Then, the location information provider forwards the information to the end-user; the information is determined by various techniques (e.g., A-GPS [5], ultrasound [6] and RSSI based on RF [7,8]). By sending a periodical location query to the base station, the end-user can obtain the location of his/her child and verify the risk of the child.

The location information of the child is encrypted by the shared key between the child and end-user so that the location service provider cannot obtain the exact location information. When the end-user wants to stop the service, he/she can deregister the service. Therefore, our conceptual model can provide the end-user with a capability of controlling the service. Fig. 3 depicts these activities.

Compared to the previous model, our approach has the following advantages. We can prevent the service provider from obtaining the private information of an end-user (e.g., location of his/her child, safety zone and frequent visiting place). This is because the service provider can only issue an authorized credential used to preserve the anonymity of the end-user. The end-user can register and deregister the service whenever he/she wants.

As the end-user in u-City may have various devices and want to experience by a seamless location supporting service, we should support various location determination techniques to deal with the mobility of the end-user. That is why we propose a conceptual model for a privacy-preserving location supporting protocol.

3.2. Our system model based on a sensor network

We choose the sensor network to be our location determination technique for the following reasons. As the sensor network will be deployed to monitor nearby environmental conditions in u-City, our system model can reuse the existing

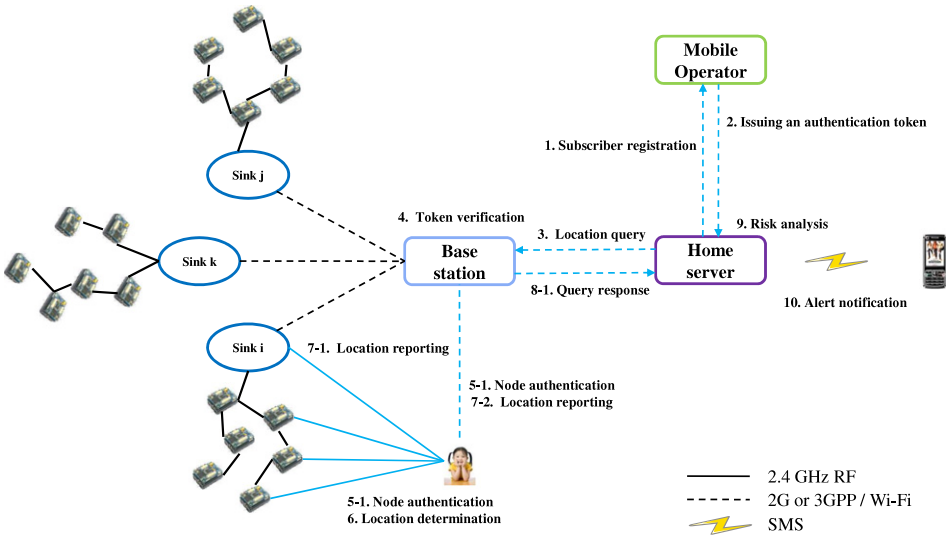

Fig. 4. Our system model.

infrastructure. In addition, a sensor node can support various cryptography primitives such as symmetric key encryption and asymmetric key encryption including pairing computations with low cost compared to a PDA, mobile phone, and wireless access point. While location determination based on the sensor network can be used indoors or outdoors, it is more accurate compared to the other techniques such as A-GPS [5] and ultrasound [6]. If the location determination technique is changed to RSSI based on Wi-Fi or UWB, our system model does not require any modification.

Fig. 4 shows our concrete system model. In this model, the sensor network consists of sink nodes, sensor nodes, and a base station. A sensor node, having battery power, gathers the nearby environmental information and sends the information to a sink node. Then, the sink node, having permanent power and the capability of direct communication with the base station, aggregates the received information and forwards it to a base station. Thus, the administrator in the base station only requires recharging a node's battery or redeploying another sensor node whenever the battery of the sensor node is exhausted. In addition, this approach can reduce unnecessary energy consumption of the intermediate nodes between a child's device and the base station, caused by forwarding authentication or service requests to the base station. As a result, our system model can increase the lifetime of the sensor network.

The base station verifies whether the end-user is a legitimate subscribers or not. To support this verification, we adopt an anonymous authentication technique based on a blind signature [12]. Only if the end-user is legitimate and registers the location query of his/her child does the base station store the received authorized credential and the child's location in its database; the location information is encrypted with a shared key between the child's device and the end-user's home server.

Also, by increasing the transmission power, a device of an end-user's child can directly communicate with the sink node via another radio frequency, which is not used by the communication between the sensor nodes and the nearby sink node. To support scalability, we should consider that the inhabitants in a city can access the sensor network using several devices. If we do not reflect this situation, the sensor network cannot achieve its primary goal such as monitoring the nearby environment but forwarding the received authentication request. As the child's device takes the role of location determination and identifies his/her location from the periodic or event message of the legitimate sensor nodes, the sensor nodes do not need any additional cost such as computations or communication. Thus, our system model can maximize the usage of the sensor network.

Finally, our system model includes the home server of the end-user to preserve the end-user's privacy, as in the system proposed by Takata et al. [10]. Using the location information received from the base station, the home server takes the role of identifying whether the end-user's child is in a safety zone. The home server periodically sends a query message including the registered credential in the location query phase. Only if the query message includes the registered credential and the message is encrypted with the shared key between the base station and end-user can the home server receive the child's location information from the base station.

3.3. Assumptions and notation

Here, we describe the assumptions used in this paper. We summarize our notation used throughout this paper in Table 1.

First, we assume that an end-user can control the source addresses of the outgoing medium access control (MAC) frames since this assumption is a prerequisite for anonymous communications. Gruteser et al. [13] covered a detailed method for this modification, but it is out of the scope of this paper. Also, the end-user distributes a fresh session key $K_{U,\mathrm{BS}}$ to his/her home server and the child's device to authenticate themselves to the base station.

Table 1
Notations.

Notation	Description
BS/MO/SN	Base station/mobile operator/sink node
Credential	End-user/a ticket for entity authentication
U/HS/KD/LDT	End-user/Home server/Child's device/location determination technique
N/ID_A	An end-user's access frequency/an identifier of entity A
PK_A or SK_A	A public key or private key of entity A
S	A set of selected numbers the length of which should be larger than $2 \cdot N$
C^i or C^i_A, $1 \le i \le n$	A series of authorized credentials
CertA	A certificate that binds entity A with A's public key
j^i or j^i_A, $1 \le i \le n$	A series of an end-user's number selections
$K_{A,B}$	A shared secret key between entities A and B
$m_1 \parallel m_2$	A message concatenation of message m_1 and m_2
$E\{m, K_A\}$	A message m is encrypted by a symmetric key K_A
$E[m, \mathrm{PK}_A]$	A message m is encrypted by an entity A's public key
$D[m, \mathrm{SK}_A]$	A message m is decrypted (or signed) by an entity A's private key
$H(m)$	A hash value of message m using a hash function such as SHA-1
R^i or R^i_A, $1 \le i \le n$	A series of 64-bit nonces generated by entity A

Second, the base station has a public key of the mobile operator $\mathrm{PK}_{\mathrm{MO}}$ and its certificate $\mathrm{Cert}_{\mathrm{MO}}$ to verify the authorized token of an end-user. In addition, the base station distributes K_{Init}, used to support message integrity in the device authentication phase, to all sink nodes in the sensor network. Although this approach is vulnerable to node compromise attack, an adversary having K_{Init} cannot deplete the batteries of other sensor nodes due to direct communication between the sink node and the base station.

Third, all sensor nodes broadcast their location information in a periodic data reporting message. Although this creates an additional two bytes of transmitting message, this approach can enable an administrator of the base station to identify which sensor nodes should be recharged. In addition, this approach can reduce the communication cost of a child's device to determine his/her location.

Finally, the end-user's child has a device equipped for communicating with sensor nodes such as Mica2, Mica2dot, and Telosb. Moreover, the device communicates with its nearby sink node using a different radio frequency compared to the radio frequency used in the sensor network. This assumption can reduce the possibility of message collision between legitimate sensor nodes and the end-users' child devices.

3.4. Our protocol

Our protocol for a child-care and safety service consists of subscriber registration, location query, device authentication, location determination, query response and location information transmission. We now describe our child-care and safety service in detail.

3.4.1. Subscriber registration

In the subscriber registration phase, an end-user generates an authentication token and sends the token to a mobile operator providing a child-care and safety service. Only if the end-user is a subscriber of the mobile operator does the mobile operator authorize the received authentication token. We illustrate this procedure in Fig. 5. To provide anonymous authentication for preserving an end-user's privacy, we adopt the idea based on the blind signature technique in [12]. The anonymous authentication provides novel properties (e.g., enhanced security level, accountability, and non-linkability) while reducing the cost of communications and computation. That is why we employ this technique.

The end-user generates two fresh nonces and signs his/her identity together with one fresh nonce R' using his/her own private key SK_U. Then, the end-user computes an anchor value C^0 using the signature. Note that this procedure can be done off-line.

When a mobile operator receives a request for subscriber registration, the mobile operator verifies the received certificate Cert_U, the end-user's identity ID_U, and the anchor value C^0 using $\mathrm{SK}_{\mathrm{MO}}$ and PK_U. Only if the request has a proper private key SK_U and certificate Cert_U does the mobile operator compute $C_S = E\{C_U, \mathrm{SK}_{\mathrm{MO}}\}$ and send $E\{\mathrm{ID}_U \| \mathrm{ID}_{\mathrm{MO}} \| C_S, K_S\}$ to the end-user. After that, the end-user verifies the received ID_U and ID_{AS} and computes C_S/R''_U to obtain a valid signature pair $(C^0, D[C^0, \mathrm{SK}_{\mathrm{MO}}])$.

As the legitimate end-user can provide a proper Cert_U and the knowledge of SK_U to the service provider, the mobile operator can authenticate the end-user. However, an adversary cannot obtain K_S, C^0 and the knowledge of SK_U due to the message encryption $\mathrm{PK}_{\mathrm{MO}}$. Also, the end-user can authenticate the mobile operator with K_S. The key K_S is shared with a legitimate mobile operator having $\mathrm{SK}_{\mathrm{MO}}$. Hence, we believe that our protocol can support mutual authentication between the end-user and the service provider.

3.4.2. Location query

In the location query phase, the end-user registers his/her authorized token with the base station. In addition, the end-user can control the child-care and safety service by registering or deregistering his/her token to the base station. This

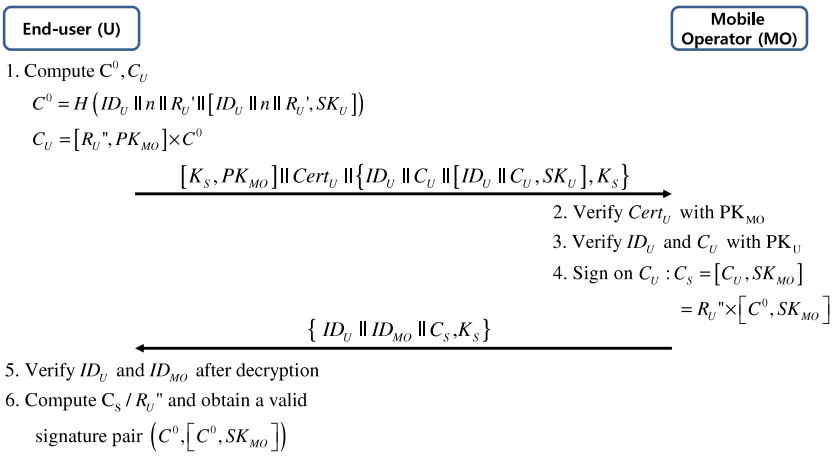

Fig. 5. Subscriber registration phase.

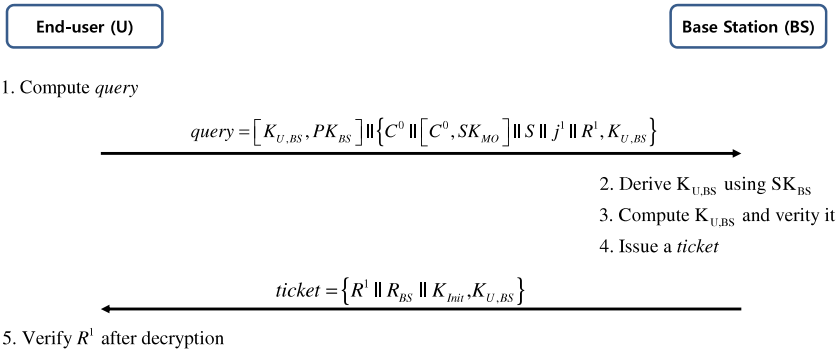

Fig. 6. Location query phase.

approach can remove the end-user's concern about illegal tracking by the mobile operator or base station. Fig. 6 depicts the location query phase.

For a location query, the end-user randomly generates a fresh nonce R^1 and a set of selected numbers S, expressed as an l-bit array. If the i-th value of S is 1, it indicates that i is already selected. Also, the end-user selects one random number j^1 between 0 to $l-1$ until the j^1-th value of S is 0. Next, the end-user computes a one-time credential $C^1 = H(C^0 \| j^1 \| R^1)$ and a session key $K_{U,BS} = H(C^0 \| PK_{BS} \| R^1 \| j^1)$. Then, the end-user sends a query message $E[K_{U,BS}, PK_{BS}] \| \{C^0 \| E[C^0, SK_{MO}] \| S \| j^1 \| R^1, K_{U,BS}\}$ to the base station.

After decrypting the received query message with SK_{BS}, the base station derives $K_{U,BS}$ and obtains the necessary information (i.e., C^0, R^1, and j^1) to compare the computed $K_{U,BS}$ with the derived one. Only if the verification result is correct does the base station compute $C^1 = H(C^0 \| j^1 \| R^1)$, send a ticket $E\{R^1 \| R_{BS} \| K_{Init}, K_{U,BS}\}$ to the end-user, and store the derived information (i.e., C^0, R^1, j^1, C^1, R_{BS}, and $K_{U,BS}$) in its database.

After decrypting the received ticket, the end-user verifies whether the derived R^1 is the same as the stored R^1. If the verification result is correct, the end-user stores K_{Init} on his/her child's device. Otherwise, the end-user retries this phase. After registration of the location query, the end-user is ready to receive the location information of the child. Whenever the child's device performs the location determination procedure, the device sends the location information to the base station via its nearby sink node.

3.4.3. Device authentication

Device authentication is required to share a fresh session key, K_S, between the child's device and its nearby sink node. Using the key K_S, the device can securely communicate with its nearby sink node and authenticate itself to the sink node without any participation of the base station.

In device authentication, a device owned by the child sends its authorized credential with necessary information for the next authorized credential to the base station via its nearby sink node. The nearby sink node forwards the received message to the base station only if the HMAC (keyed-hash message authentication code) of the received message is valid.

Then, the base station checks the integrity of the received authentication token. Only if the verification result is correct does the base search $K_{U,BS}$ in its database using C^{i-1}, where $i = 2, 3, \ldots, n$. Using the found $K_{U,BS}$, the base station decrypts

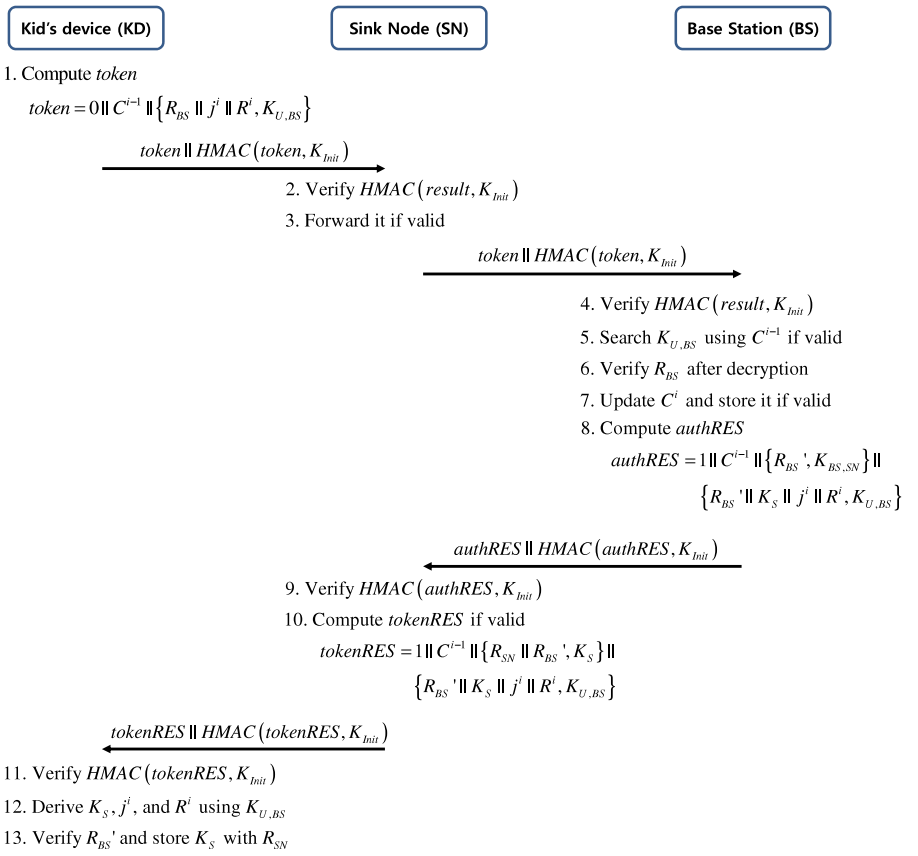

Fig. 7. Device authentication phase.

the token and verifies R_{BS}. If the verification is correct, the base station authenticates the device, updates $C^i = H(C^0 \| j^i \| Ri)$, and stores C^i in its database, where i indicates the i-th authentication request. Otherwise, the base station drops the received token. Note that the base station has C^0, R^1, j^1, C^1, R_{BS}, and $K_{U,BS}$ in its database after the location query phase. Also, this information is only known to the end-user and the base station. As a result, the base station can identify that the device is legal and authorized. After storing the updated C^i, the base station computes a response message of the received token, called *authRES*, and forwards *authRES* to the nearby sink node of the device. Note that K_S is $H(R'_{BS} \| K_{CK})$, where K_{CK} is a shared key between the nearby sink node and its members consisting of a cluster for data aggregation.

The nearby sink node verifies the integrity of the received message, computes a response message of the received token, called *tokenRES*, and sends it to the device.

After receiving *tokenRES* and verifying its integrity, the device derives K_S, j^i, and R^i using $K_{U,BS}$. Only if the received R'_{BS} from the base station and the received R'_{BS} from the nearby sink node are the same does the device store K_S and R_{SN}. We illustrate this procedure in Fig. 7.

When the device supports a capability of accessing a Wi-Fi or 3GPP network, the device sends the *token* directly to the base station. The only difference with the procedure in Fig. 7 is the message $E\{R'_{BS}, K_S, j^i, R^i, K_{U,BS}\}$ directly sent by the base station to the device. Since the bandwidth of Wi-Fi and 3GPP networks is higher than that of the sensor network, this approach can reduce the processing delay and support better scalability.

Although the base station has K_S, the key that is shared with the child's device, the base station cannot identify the owner of the device. In the location query phase, the base station only verifies the legitimacy of the received token. When the token is authorized by the mobile operator, the base station stores K_S and C^0 in its database. Therefore, we believe that our protocol can support the privacy of the end-user by hiding the relationship between the device and the end-user.

3.4.4. Location determination

Since the device owned by a child has K_{Init} and K_S, the device can distinguish whether the nearby sensor nodes are members of the sensor network belonging to the base station.

Using triangulation based on RSSI [7] from three or more legitimate sensor nodes, the device can determine its location within 3 m. As our interest is not the location determination technique, a detailed method is out of scope in our paper. After identifying the location of the device, the device broadcasts a result message $R_{SN} \| C^{i-1} \| E\{\text{ZONE} \| R_{KD} \| R_{BS}, K_{HS,KD}\}$ with its HMAC to its nearby sink nodes.

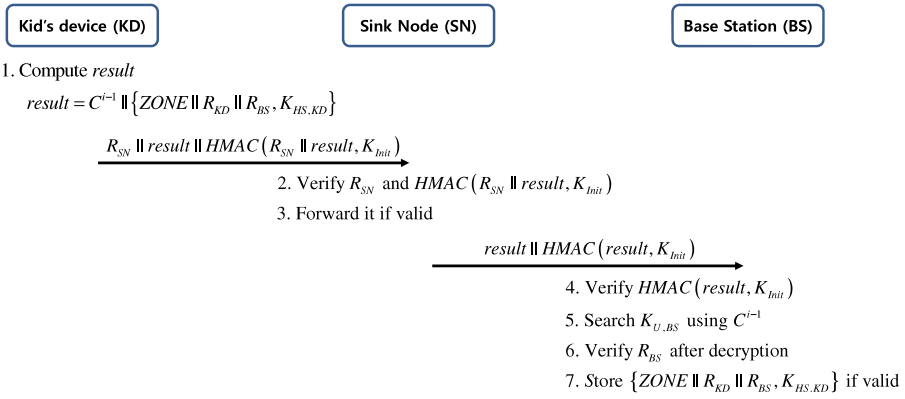

Fig. 8. Location determination phase.

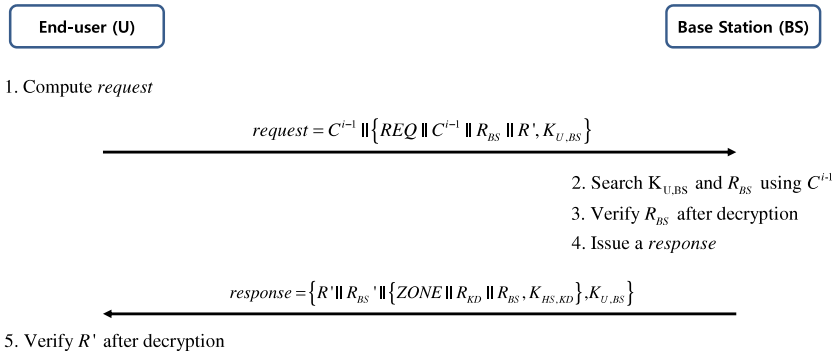

Fig. 9. Location response phase.

The nearby sink node verifies the integrity of the received message and checks whether the device has the proper R_{SN} and C^{i-1}. Only if the device has valid R_{SN} and C^{i-1} does the sink node forward the received message to the base station.

The base station verifies the integrity of the received message, searches $K_{U,\mathrm{BS}}$ in its database using C^{i-1}, decrypts the message, and verifies R_{BS} using $K_{U,\mathrm{BS}}$. If the verification result is correct, the base station stores $E\{\mathrm{ZONE}\|R_{\mathrm{KD}}\|R_{\mathrm{BS}}, K_{\mathrm{HS,KD}}\}$ in its database. Otherwise, the base station drops the received message. Fig. 8 illustrates this procedure. When the device can directly access the base station through Wi-Fi and 3GPP, the *result* message is sent directly to the base station. As a result, the nearby sink node can handle more messages from the child's device by reducing the processing time of the received message in the nearby sink node. That is why we believe that our protocol can support better scalability.

3.4.5. Query response

In the query response phase, an end-user sends a location request $C^{i-1}\|E\{REQ\|C^{i-1}\|R_{\mathrm{BS}}\|R', K_{U,\mathrm{BS}}\}$ to the base station via his/her home server, where R' is a fresh nonce and REQ is the message type.

The base station stores the location information of the child, $K_{U,\mathrm{BS}}$, C^i, j^i, R^i, and C^0, in its database. Using the stored C^{i-1}, the base station can find the necessary information (i.e., $K_{U,\mathrm{BS}}$ and R_{BS}) and compare the received R_{BS} with the stored R_{BS}. Only if the result is correct and the location information is received from the device does the base station issue and send a response $R'\|R'_{\mathrm{BS}}\|E\{\mathrm{ZONE}\|R_{\mathrm{KD}}, K_{\mathrm{HS,KD}}\}$ to the end-user.

The end-user's home server decrypts the received response and verifies R' with $K_{U,\mathrm{BS}}$. Only if the verification result is correct can the home server start to identify the child's location. Otherwise, the home server retries the query response phase. Fig. 9 shows this procedure.

3.4.6. Location information transmission

After receiving the query response from the base station, the home server can identify the child's location. If the location is in a dangerous area, the home server sends an alerting message to the end-user's mobile phone. If the end-user wants to observe the child's location periodically, the home server can send the location information to the end-user's mobile phone.

3.5. Our system model over a Wi-Fi network

Since various Wi-Fi-based smart phones are popular and the mobile operators have their own Wi-Fi networks, we illustrate an example scenario with a Wi-Fi-based mobile device in Fig. 10.

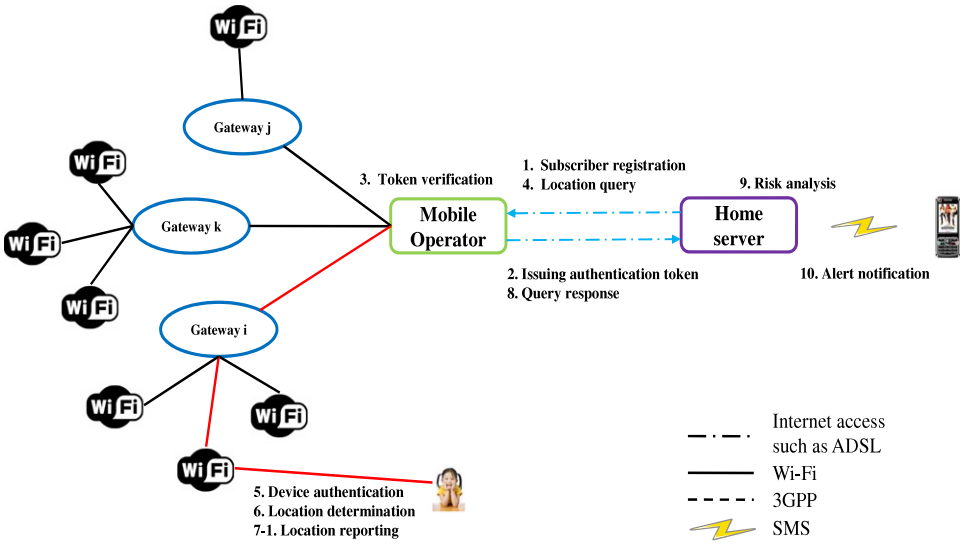

Fig. 10. An example scenario with a Wi-Fi-based mobile device.

Table 2
Properties comparison.

Properties	Existing services in Korea	Takata et al. [10]	Ours
Risk analysis	By service provider	By end-user	By end-user
LDT	GPS	GPS	RSSI based on RF
Accuracy	∼2 km (outdoor) ∼10 m (indoor)	∼2 km (outdoor) ∼10 m (indoor)	∼3 m
Supporting area	Indoor and outdoor	Indoor and outdoor	Indoor and outdoor[a]
Cost	High	High	Medium
Direct communication	Not required	Required	Not required
Infrastructure	Required	Not required	Required
Privacy protection	X	O	O
Controllability of an end-user	X	O	O

[a] An area supporting RF communication.

Compared to our system model in Fig. 4, the only differences are that the mobile operator takes the role of location service provider and the device cannot directly communicate with the mobile operator. This is because we should prevent the mobile operator from identifying the end-user although the mobile operator can identify the device owned by a child.

4. Analysis of our protocol

Since the existing approaches are GPS based, the performance comparison between our protocol and the previous approaches is not meaningful. That is why we only show a properties comparison in Table 2. The existing services in Korea employ an assisted GPS to determine an end-user's location whether the end-user is indoors or outdoors. Although the services have 10 m accuracy in outdoor environments, the accuracy of the services is changed to 2 km in indoor environments. Since the signal strength of the GPS is too weak for location determination in an indoor environment, the accuracy of the GPS does not influence the accuracy of the service in an indoor environment.

In our protocol, the child's device only requires an RF communication module whereas the device in previous work should include a GPS module and any communication module (e.g., 3G network and Wi-Fi). Even if our protocol requires the existing infrastructures such as a wireless sensor network and Wi-Fi, our protocol maximizes the usage of the infrastructures and reduces the computation and communication cost of the infrastructures. Hence, we believe that our approach is useful in u-City.

By deploying several access points (i.e., sink nodes in our protocol), our protocol can provide a child-care and safety service in an outdoor environment. Although this approach incurs an additional deployment cost, the cost may be less than the all subscribers' expenditures for their GPS modules in the outdoor environment. Also, in u-City, these access points may be deployed to support seamless connection for the subscribers.

In our performance analysis, we illustrate the efficiency of our protocol. Specially, our protocol supports scalability by reducing the computation and communication overhead of the existing infrastructure. A sink node requires only one symmetric key operation and 8 hash operations for device authentication and the location determination phase while the deployed sensor nodes do not require any computation and communication cost. Also, in our security analysis, we

Table 3
Computational overhead in each phase.

Phase	Entity	Public key oper.	Sign. oper.	Symmetric key oper.	Hash oper.
Subscriber	U	2 (off-line)+1	1 (off-line)	2	1
Registration	MO	1	2	2	1
Location	U	1 (off-line)	0	1	1
Query	BS	1	1	1	1
	KD	0	0	3	5
Device authentication	SN	0	0	1	6
	BS	0	0	3	5
	KD	0	0	1	2
Location determination	SN	0	0	0	2
	BS	0	0	0	2
Location	U	0	0	3	0
Response	BS	0	0	2	2

Oper.: Operation, Sign: Signature.

Table 4
Communication cost of a child's device.

		Communication cost	
		(μJ)	(bytes)
Device	E_{tx}	0.99840000	72
Authentication	E_{rx}	1.08160000	104
Location	E_{tx}	1.10933333	80
Determination	E_{rx}	0	0
Device authentication	E_{tx}	0.12343333	89
Based on B-MAC [11]	E_{rx}	1.25840000	121
Location determination	E_{tx}	1.3450666	97
Based on B-MAC [11]	E_{rx}	0	0

indicate that our protocol can satisfy the security requirements of a child-care and safety service in a ubiquitous computing environment.

4.1. Performance analysis

Storage cost: A device owned by an end-user's child is only required to save R_{KD}, R_{BS}, C^0, R^i, j^i, n, S, $K_{U,BS}$, $K_{HS,KD}$, and the shared key between the device and its nearby sink node, K_S. Since C^l, where l is 1, . . . , n, can be generated directly from the anchor value, this means that our protocol does not require us to store all credential information.

Computational cost: We present the computational cost of each phase in Table 3. If an "off-line" entry exists, the computation can be done prior to the session. For instance, an end-user should require online computation (one public key operation, two symmetric key operations, and one hash operation) and off-line computation (two public key operations and one signature generation) in the subscriber registration phase. Since a child's device in our protocol requires only symmetric key operations and hash operations, we believe that our protocol can support various devices with the limited resources in a ubiquitous computing environment.

Communicational cost: In our protocol, for device authentication, the device owned by an end-user's child requires only two rounds, which is the minimum number of rounds to achieve authenticated key establishment protocol. In addition, the device requires one round to report the child's location. From this, we believe that our protocol is lightweight in the number of communication rounds.

To compute the lifetime of a child's device, we assume that AES-128 and SHA-1 are used as the symmetric encryption scheme and the hash function. Also, we assume that n is 80 and that the message transmission rate r is every 30 min (i.e., 1/(30 min $*$ 60 s) packet/sec). Based on the analytical model in [11], we compute the total energy consumption of the device for a regular location report and illustrate the result in Table 4. Note that z is 1 since the child's device can directly communicate with a nearby sink node, indicating that E_{tx} is independent of neighbor size. Also, we only consider the necessary message for our protocol in the above computation. When we adopt B-MAC [11], one of the efficient MACs for wireless sensor networks in the literature, an additional 17 bytes (i.e., 8 bytes for the preamble, 2 bytes for synchronization, 5 bytes for the header, and 2 bytes for the CRC) are required, and we present the total energy consumption of the device for a regular location report in Table 4.

Since the device consumes 3.18933333 μJ without B-MAC (or 3.83760000 μJ with B-MAC), our protocol satisfies lightweightness.

4.2. Security analysis

Mutual authentication: In our protocol, an end-user including the device owned by the end-user's child authenticates him/her to the base station (or mobile operator) using the authorized credential, so that the base station (or mobile operator)

knows that the user is legal and authorized. The base station (or mobile operator) authenticates itself to the user through its own public key and by showing its knowledge of the corresponding private key.

Privacy protection: Since any private information (e.g., safety zone, mobile phone number, and location information) are stored in the personal home server, the mobile operator only issues an end-user's authorized credential for anonymous authentication, and the base station verifies the authorized credential with PK_{MO}, an administrator at the mobile operator cannot obtain any private information during a location query, location determination, and query response.

Moreover, an administrator in the base station cannot distinguish who requests the child-care and safety service due to anonymous authentication. Note that the base station can guess the child's nearby location since the information is delivered to the base station via a nearby sink node. However, the base station cannot find any relationship between the location information and the end-user. Hence, our service can preserve an end-user's privacy.

Also, the privacy of the end-user's child can be protected as the end-user and his/her parents can control his/her location information transmission.

Confidentiality and integrity: All communications are encrypted with a receiver's public key or symmetric key, which is shared between the sender and the receiver. Thus, confidentiality is provided in our service. Also, the sender and receiver can derive a secret key for the HMAC using the shared key. Hence, integrity can be easily provided in our service.

Scalability: Since our protocol can support anonymous authentication based on the authorized credential, our protocol may be vulnerable to battery exhaustion attack, sending continuous or periodic authentication requests (or location reporting). As the base station can only verify an end-user's authentication request, the intermediate nodes between an adversary and the base station should forward the received message to their parent node. That is why a battery exhaustion attack is possible. However, we reduce the effective bounds of a battery exhaustion attack to one of the adversary's nearby clusters based on the following observations. First, an outsider cannot generate a valid authentication request since the outsider does not know K_{Init}. Second, a sink node, having a permanent power for ease of network management, can directly communicate with the base station to minimize the hop distance between the adversary and the base station although the adversary has K_{Init} by compromising one of sensor nodes. Third, we assume that a child's device communicates with its nearby sink node via a different radio frequency from the one used in communication between the sensor node and the sink node. Therefore, we believe that our protocol can provide scalability.

Lightweightness: In our protocol, a child's device only needs four symmetric key operations, three HMAC operations, and one hash operation, for device authentication and location determination. Also, the device does not require communicating with the child's home server. Hence, our protocol is believed to be more lightweight than the previous approach [10].

5. Conclusion

In this paper, we propose a privacy-preserving location supporting protocol for child-care and safety in a ubiquitous computing environment. Our main contribution is to preserve the privacy of an end-user while enhancing the accuracy of the child's location to 3 m. Although we employ triangulation based on RSSI [7] from three or more legitimate sensor nodes in the specific technique of our location determination, various techniques such as Wi-Fi RSSI and WLAN RSSI can be applied to our protocol without any modification if the device of the target child supports Wi-Fi and WLAN. By restricting the role of the child-care and safety service provider to issuing an authorized credential for an end-user's anonymity, the end-user can preserve his/her private information. The end-user can register and deregister the service whenever he/she wants. In previous approaches, the end-user could not deregister the service until he/she is a legitimate subscriber of the child-care and safety service.

Our protocol delegates the role of location determination to a child's device so that the deployed sensor nodes do not require authenticating the child's device for location determination. Through reducing the energy consumption of the deployed nodes due to communication cost, we believe that our protocol can support better scalability. In addition, we show the efficiency of our protocol by illustrating the storage, computation and communication cost. The child's device only requires symmetric key operations and hash operations. Finally, our approach needs less deployment cost by maximizing usage of the deployed sensor network.

In the near future, we will implement our service on sensor nodes for rigorous analysis. Also, for a security framework in u-City, we will combine this work with a secure service discovery protocol, which is necessary in u-City.

References

[1] Cyberport home page. http://www.cyberport.com.hk/cyberport/en/home/home_flash.html (accessed 17.12.09).
[2] u-Seoul home page. http://u.seoul.go.kr/ (accessed 17.12.09) written in Korean.
[3] Knowledge capital project home page. http://kita-yard.com/en/kc/index.html (accessed 17.12.09).
[4] u-safe Gangnam home page. http://usafe.gangnam.go.kr/u-safe_01.html (accessed 17.12.09), written in Korean.
[5] Assisted GPS, Wikipedia. http://en.wikipedia.org/wiki/Assisted_GPS (accessed 17.12.09).
[6] N. Priyantha, A. Chakraborty, H. Balakrishnan, The cricket location-support system, in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, USA, August 6–11, 2000, pp. 32–43.
[7] P. Bahl, V.N. Padmanabhan, RADAR: an in-building RF-based user location and tracking system, in: Proceedings of IEEE Infocom 2000, Tel Aviv, Israel, March 26–30, 2000, pp. 775–784.
[8] G.V. Zàruba, M. Huber, F.A. Kamangar, I. Chlamtac, Indoor location tracking using RSSI readings from a single Wi-Fi access point, Wireless Networks 13 (2007) 221–235.

[9] Cognition against social safety, 2008 database. http://www.kosis.kr/ (accessed 17.12.09) written in Korean.
[10] K. Takata, J. Ma, B.O. Apduhan, A dangerous location aware system for assisting kids safety care, in: 20th International Conference on Advanced Information Networking and Applications, Vienna, Austria, April 18–20, 2006, pp. 657–662.
[11] J. Polastre, J. Hill, D. Culler, Versatile low power media access for wireless sensor networks, in: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA, November 3–5, 2004, pp. 95–107.
[12] J. Kim, Z. Kim, K. Kim, A lightweight privacy preserving authentication and access control scheme for ubiquitous computing environment, In: Proceedings of 10th International Conference on Information Security and Cryptology, Seoul, Korea, November 29–30, 2007, pp. 37–48.
[13] M. Gruteser, D. Grunwald, Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis, Mobile Networks Applications 10 (2003) 315–325.