SCIS 2010 The 2010 Symposium on Cryptography and Information Security
Takamatsu, Japan, Jan. 19-22, 2010
The Institute of Electronics, Information and Communication Engineers

A privacy-preserving kid's safety care service based on sensor network in u-City

Jangseong Kim * Myunghan Yoo * Kwangjo Kim *

Abstract— Although several mobile operators such as SKT, KTF, and LGT in Korea provide their own kid's safety care services to reduce many parents' concern, three problems still remain: incorrect location information, privacy violation, and no capability of an end-user to control the safety care service during access to the service.

In this paper, we derive security requirements of kid's safety care service and explain our system model to satisfy these requirements. Based on our system model we propose our protocol for kid's safety care service. Compared to the previous work, our protocol can enhance accuracy of location information, preserver privacy of an end-user, and give an end-user a capability controlling the safety care service during access to the service.

Keywords: kid's safety care, sensor network, u-City

1 Introduction

Recently, ubiquitous technologies such as RFID and sensor network are becoming one part of our lives. One of typical examples is ubiquitous IT city (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 (*i.e.*, ubiquitous port, ubiquitous health care, ubiquitous office, ubiquitous safety). Several cities such as Hong Kong [1], Seoul [2], and Osaka [3] have a plan to introduce these technologies into our lives and concrete the plan.

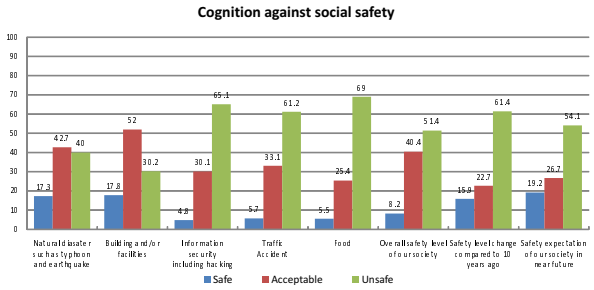

Figure 1: Cognition against social safety [4]

Compared to 10 years ago, 61.4% people in Korea realize that safety level changes to unsafe as shown in Fig. 1. Also, as a heinous crime against kid increases, many parents worry about their kid's safety during commuting to a school or playground near their home. Moreover, 54.1% people expect that safety level of our society becomes to unsafe in near future. Therefore, u-City which will appear soon should provide safety care service to its inhabitants. To address this situation, mobile service providers such as SKT, KTF, and LGT provide their own kid's safety care service and the subscriber of these services are continuously increasing. In addition, Gangnam province in Seoul provides 'u-safe Gangnam' to its inhabitants for kid's safety care, disabled person, and elder person who live alone from May, 2009 [5]. However, their approaches has several problems: the location information is incorrect location due to the number of deployed stations and technology limitation; privacy of an end-user can be violated by private information stored in a server of service provider; and an end-user cannot control over these services. In this point, these services cannot satisfy demand of inhabitants in u-City.

In this paper, we propose a privacy-preserving kid's safety care service using the sensor network deployed in u-City. Through location determination based on sensor network, we can enhance accuracy of location determination. Also, our approach needs less deployment cost by maximizing usage of the deployed sensor network. To preserve privacy of an end-user, we limit a role of mobile service provider to issue an authorized credential for an end-user's anonymity and delegate a role of location determination to a kid's device. In addition, the end-user can control safety service for his/her kid whenever the user wants.

The organization of this paper is as follow: in Section 2, we discuss with the related work, system model, and security requirements; Then, we present our proposed service in Section 3 and analyze its security analysis in Section 4; Finally, we conclude this paper with short summary in Section 5.

* KAIST, 103-7 Munjidong, YuseongGu, Daejeon, 305-732 Korea
{jskim.withkals, bishnu, kkj@kaist.ac.kr}

2 Related work and security requirement

We discuss several approaches for kid's safety care services with their disadvantages. Also, we clarify security requirements of kid's safety care service.

2.1 Related work

In Korea, mobile service providers (*i.e.*, SKT, KTF, and LGT) provide kid's safety care service. The service providers notify a kid's location information to parents' mobile phone per every 1 hour and send an alarm message if a kid is out of his/her safety zone, predetermined by the kid's parent. However, this approach has the following disadvantages: the kid's location is not accurate due to A-GPS (Network-assisted GPS) [6], typical method of location determination technology; Private information such as safety zone and mobile phone should be stored in a server of mobile operator; An end-user cannot control over kid's safety care service although the user does not want to observe his/her kid's location during some time period. Also, Gangnam province in Seoul provides a similar service to an end-user.

In the open literature, Takata *et al.* [7] proposed a dangerous location aware system for assisting kids safety care. To assist for kid's safety care, they assume that each kid has proper mobile devices communicating with a server in his/her home and a public alerting service notifying several dangerous location 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 kid's location in the kid's device. However, direct communication between the kid's device and home server in his/her home is expensive and impractical since the devices should support various networking technologies as any changes of the nearby environment. From this, we believe that their approach is not proper in u-City.

2.2 Security requirement

Kid's safety care service should satisfy the following requirements: mutual authentication, privacy protection of an end-user, confidentiality, integrity, and lightweightness.

Mutual authentication: Mutual authentication is required since each end-user and service provider want to identify whether the communicating party is 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 a 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 kid's safety care service enforces an end-user to store private information (*i.e.*, safety zone and mobile phone number) to 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 over the kid's safety care service although the user do not want to observe his/her kid's location during some time period. This situation helps that the adversary tracks the end-user because the malicious administrator of the service provider can expose the kid's location to the adversary. Hence, privacy of an end-user should be protected.

Confidentiality and integrity: The exact location information should be only known to the kid's parent. Thus, the location information should be encrypted with a key, which is only known to the kid's parent. Location information can be modified unless the kid's safety care service does not support integrity. Thus, confidentiality and integrity should be provided.

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

3 Our protocol

In this section, we describe our system and protocol for kid's safety care service in detail.

3.1 Our system model

To satisfy these security requirements in section 2, we propose the following system model. As sensor network will be deployed to monitor nearby environmental condition in u-City, our system model can reuse the existing infrastructure. In addition, a sensor node can support various cryptography primitives such as symmetric key encryption, asymmetric key encryption including pairing computations with low cost compared to PDA, mobile phone, and wireless access point. Even if location determination based on sensor network can be used for indoor or outdoor, it is more accurate without GPS receiver or ultrasonic transmitter/receiver. Thus, sensor network is one of possible solution for location determination u-City.

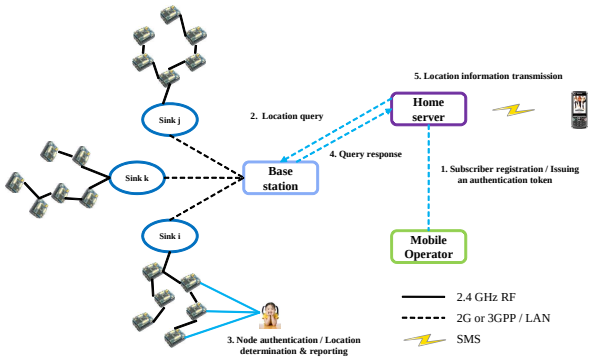

Figure 2: Our system model

Fig. 2 shows our system model. In this model, sensor

Table 1: Notation

BS	Base Station
$Credential$	A ticket for authentication
HS	Home server
KD	Kid's device
MO	Mobile Operator
n	A user's access frequency
PK_A	A public key of entity A (*e.g.*, PK_{MO} is a public key of a mobile operator)
S	A set of selected numbers which length should be larger than $2n$
SK_A	A private key of entity A (*e.g.*, SK_{MO} is a private key of a mobile operator)
SN	Sink node
U	End-user
ID_A	An identifier of entity A (*e.g.*, ID_U is identifier of an end-user)
$m_1 \| \| m_2$	A message concatenation of message m_1 and m_2
$C^i, i = 0, 1, \cdots$	A series of authorized credentials
$j^i, i = 1, 2, \cdots$	A series of a user's number selections
$Cert_A$	A certificate which binds entity A with A's public key
$E\{m, K_A\}$	A message m is encrypted by a symmetric key K_A
$E[m, PK_A]$	A message m is encrypted by public key of entity A
$D[m, SK_A]$	A message m is signed by private key of entity A
$H(m)$	Hashing a message m
$K_{A,B}$	A shared secret key between entities A and B
$R_A^i, i = 1, 2, \cdots$	A series of nonce generated by entity A which is usually a 64-bit pseudo random number.

network consists of sink nodes, sensor nodes, a base station. A sensor node gathers the nearby environmental information and sends the information to a sink node. Then, the sink node aggregates the received information and forwards it to a base station. Compared to a sensor node having a battery power, a sink node has a permanent power for easiness of network management. Whenever the battery of a sensor node is exhausted, the administrator will recharge the node's battery or deploy another sensor node. As the system model proposed by Takata *et al.* [7], our system model includes a home server of an end-user to preserve privacy of the end-user. Using the location information received from the base station, the home server takes a role of identifying whether the end-user's kid is in safety zone. We divide the role of mobile operator into two parts: infrastructure for location determination and entity authentication. By dividing the role of mobile operator, we can obtain three advantages: first, we can prevent mobile operator from obtaining location information of the end-user's kid; second, we forbid mobile operator from identifying who requests location query; third, several mobile operators can share the sensor network.

3.2 Notation

We summarize the notations used throughout this paper in table 1.

3.3 Assumptions

Here, we describe our assumptions used in this paper.

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.* [8] covered a detailed method for this modification, but it is out of scope of this paper. Also, the end-user distributes a fresh session key to his/her home server and kid's device to prevent other entities from obtaining location information.

Second, the base station has a public key of the mobile operator PK_{MO} and its certificate $Cert_{MO}$ to verify the authorized token of an end-user. Also, the base station distributes K_{Init}, used to support message integrity and add new sensor nodes, to all sensor nodes in the sensor network. Although this approach sharing one secret key is vulnerable to node compromise attack, key update after certain time period can mitigate the effect of node compromise attack.

Third, all sensor nodes consisting of a sensor network broadcast their location information in periodic data reporting message. Although increases 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 communication cost of a kid's device to determine his/her location.

3.4 Our protocol for kid's safety care service

Our protocol for kid's safety care service consists of subscriber registration, location query, device authentication, location determination, query response, location information transmission. From now, we describe our kid's safety care service in detail.

3.4.1 Subscriber registration

In subscriber registration phase, an end-user generates an authentication token and send the token to a mobile operator providing kid's safety care service. Only if the end-user is a subscriber of the mobile operator, the mobile operator authorizes the received authentication token. Since we want to provide anonymous authentication, we adopt blind signature technique. The end-user generates two fresh nonces and signs his/her identity together with one fresh nonce R' using own private key SK_U. Then, the end-user computes an anchor value C^0 with the signature. Note that the procedure can be done off-line. We summarize it as:

1. Generate two fresh nonces: R' and R''
2. Sign user's own ID with a fresh nonce R' and n: $D[ID_U||n||R', SK_U]$
3. Compute the anchor value C^0 of credential chain as: $C^0 = H(ID_{User}||n||R'||D[ID_U||n||R', SK_U])$
4. Blind C^0 as $C_U = E[R'', PK_{MO}] \times C^0$

When a mobile operator receives a request for subscriber registration, the mobile operator verifies the received certificate $Cert_U$, end-user's identity ID_U, and anchor value C^0 using SK_{MO} and PK_U. Only if the request has proper private key SK_U and certificate, the mobile operator signs on the received C^0 with SK_{MO} and sends $\{ID_U||ID_{MO}||C_S, K_S\}$ to the end-user. After then, the end-user verifies the received ID_U and ID_{AS} and compute C_S/R''_U to obtain a valid signature pair (C^0, $[C^0, SK_{MO}]$).

We illustrate this procedure in Fig. 3.

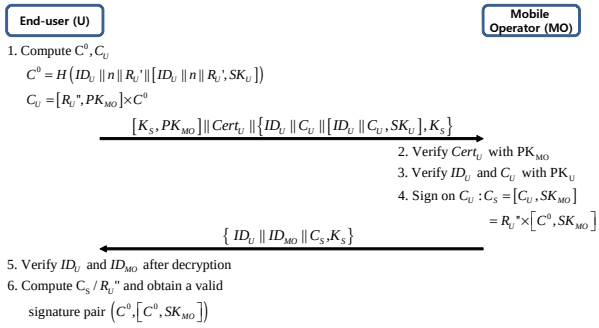

Figure 3: Subscriber registration phase

3.4.2 Location query

For location query, the end-user randomly generates a fresh nonce R^1 and a set of selected numbers S, expressed as 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 j^1-th value of S is 0. Next, the end-user computes one-time credential $C^1 = H(C^0||j^1||R^1)$ and session key $K_{U,BS} = H(C^0||PK_{BS}||R^1||j^1)$. Then, the end-user sends a query message $[K_{U,BS}, PK_{BS}]||\{C^0||[C^0, SK_{MO}]||S||j^1||R^1, K_{U,BS}\}$ to the base station.

The base station derives $K_{U,BS}$ with its private key SK_{BS} and obtain necessary information (*i.e.*, C^0, R^1, and j^1) to compare a computed $K_{U,BS}$ with the derived one. Only if the verification result is correct, the base station sends a ticket $\{R^1||R_{BS}||K_{Init}, K_{U,BS}\}$ to the end-user, computes $C^1 = H(C^0||j^1||R^1)$, and stores C^0, R^1, j^1, C^1, R_{BS}, and $K_{U,BS}$ in its database.

After decrypting ticket, the end-user verifies whether the derived R^1 is the same as sent R^1. If the verification result is correct, the end-user stores K_{Init} to his/her kid's device. Otherwise, the end-user retries this phase.

Fig. 4 depicts this procedure. After registration, the end-user can be ready to receive the location information of his/her kid. Whenever his/her kid's device performs location determination procedure, the device send location information to the base station via its nearby sensor nodes.

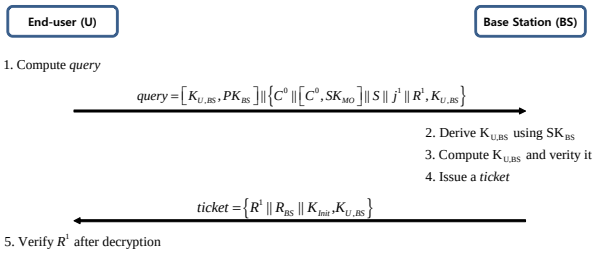

Figure 4: Location query phase

3.4.3 Device authentication

To reduce energy consumption caused by DoS (Denial-of-Service) attack, device authentication phase is required. In device authentication, a kid's device sends its authorized credential with necessary information to compute next authorized credential to the base station via its nearby sensor nodes. The nearby sensor nodes forward the received message to their sink node only if HMAC (keyed-Hash Message Authentication Code) of the received message is valid. Also, the sink node forwards the received message to the base station for device authentication.

Then, the base station checks integrity of the received authentication token and searches $K_{U,BS}$ using C^{i-1} where $i = 2, 3, \cdots, n$ only if verification result is correct. Using the found $K_{U,BS}$, the base station decrypts the received token and verifies R_{BS}. Only if verification is correct, the base station can authenticate the kid's device, update $C^i = H(C^0||j^i||R^i)$, and store it in its database. 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 location query phase. Also, this information is only known to the end-user and base station. As a result, the base station can identify that the kid's device is legal and authorized. After storing updated C^i, the base station computes a response message of the

received token, called as $authRES$, and forwards it to the nearby sink node of the kid's 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 of the kid's device verifies integrity of the received message, computes a response message of the received token, called as $tokenRES$, and sends it to the kid's device.

After receiving $tokenRES$ and verifying its integrity, the kid's devices 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, the device stores K_S and R_{SN}. We illustrate this procedure in Fig. 5.

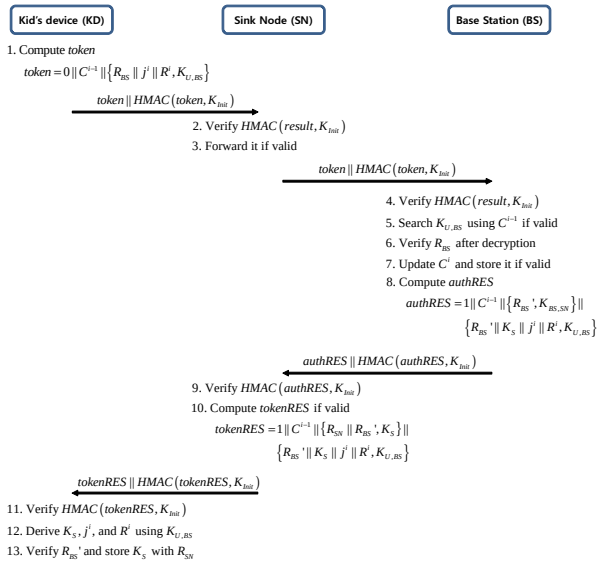

Figure 5: Device authentication phase

3.4.4 Location determination

Since the device of an end-user's kid has K_{Init}, 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 (Radio Signal Strength Indication) [9, 10] from three or more legitimate sensor nodes, the device can determine its location within 3 meters. As our interest is not location determination technique, we do not cover a detailed method in our paper. After identifying the location of the device, the device broadcasts a result message $R_{SN}||C^{i-1}||\{ZONE||R_{KD}||R_{BS}, K_{HS,KD}\}$ with its HMAC to its nearby sensor nodes.

The nearby sensor node verifies HMAC of the received message and forward it its parent node if the verification is correct. Until the message is reached to the sink node, the parent node verifies HMAC of the received message and forwards it. Then, the sink node checks integrity of the received message and checks whether the device has proper R_{SN} and C^{i-1} or not. Only if the kid's device has valid information, the received message is forwarded to the base station.

After the base station received the message, the base station verifies HMAC of the message and searches $K_{U,BS}$ in its database using C^{i-1}. Then, the base station decrypts the message and verifies R_{BS} using $K_{U,BS}$. If verification result is correct, the base station stores $\{ZONE||R_{KD}||R_{BS}, K_{HS,KD}\}$ in its database. Otherwise, the base station drops the received message. Fig. 6 illustrates this procedure.

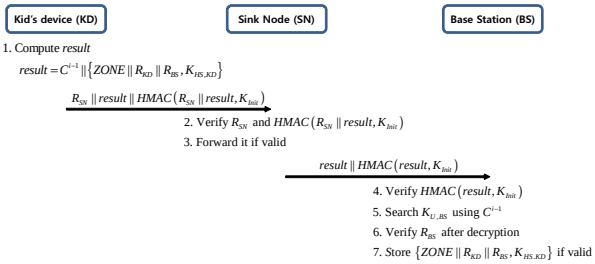

Figure 6: Location determination phase

3.4.5 Query response

In query response phase, an end-user sends a location request $C^{i-1}||\{REQ||C^{i-1}||R_{BS}||R', K_{U,BS}\}$ to the base station via his/her home server, where R' is a fresh nonce and REQ is message type. To prevent the base station from identifying the end-user, the base station stores location information of the end-user's kid in its database and sends the information to the end-user only if the user is a legitimate entity having the stored authored credential in its database.

Since the base station stores location information of the registered device, shared session key $K_{U,BS}$, authorized credential C^i, selected number j^i, nonce R^i, and anchor C^0 in its database, the base station can find $K_{U,BS}$ and R_{BS} using C^{i-1}. Then, the base station verifies the received R_{BS} with the stored R_{BS}. Only if the verification result is correct and location information is received from kid's device, the base station issues and sends a response $R'||R'_{BS}||\{ZONE||R_{KID}, K_{HS,KD}\}$ to the end-user.

The end-user's home server decrypts the received response and verifies R' with $K_{U,BS}$. Only if the verification result is correct, the home server can start to identify the kid's location. Otherwise, the home server retries query response phase. Fig. 7 shows this procedure.

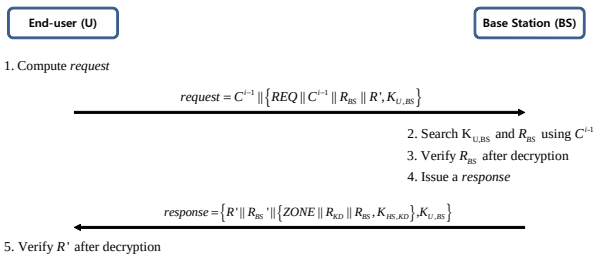

Figure 7: Location response phase

3.4.6 Location information transmission

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

4 Analysis

In this section, we analyze our kid's safety care service in security aspect.

4.1 Security analysis

4.1.1 Mutual authentication

In our protocol for kid's safety care service, an end-user including kid's device authenticates himself/herself to the base station or mobile operator using his/her own authorized credential, so that the base station or mobile operator know that the user is legal and authorized. The base station or mobile operator also authenticate themselves to the user through its own public key and by showing his/her knowledge of the corresponding private key.

4.1.2 Privacy protection

Compared to the previous work, our service can preserve privacy of an end-user. Since any private information (*i.e.*, safety zone, mobile phone number, and location information) are stored in personal home server and mobile operator takes a role of entity authentication, an administrator in mobile operator cannot obtain any private information during location query, location determination, and query response.

Also, privacy of the end-user's kid can be protected as the kid can control over his/her location information transmission. Moreover, an administrator in base station cannot distinguish who a service requestor due to anonymous authentication. Note that the base station can identify the kid's near location since location information of the requestor's kid is delivered to the kid's home server via the base station. However, the base station cannot find any relationship between the location information and the service requestor. Hence, our service preserve privacy of an end-user.

4.1.3 Confidentiality and integrity

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

4.1.4 Lightweightness

In our protocol, a kid's device only needs symmetric key operation and HMAC for location determination. Also, the device does not require to communicate with the kid's home server. Hence, our protocol is believed to be lightweight than the previous approach [7].

5 Conclusion

In this paper, we propose a privacy-preserving kid's safety care service using the sensor network deployed in u-City. Through location determination based on sensor network, we can enhance accuracy of location determination. Also, our approach needs less deployment cost by maximizing usage of the deployed sensor network. To preserve privacy of an end-user, we limit a role of mobile service provider to issue an authorized credential for an end-user's anonymity and delegate a role of location determination to a kid's device. In addition, the end-user can control safety service for his/her kid whenever the user wants.

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

References

[1] "Cyberport," Hong Kong Cyberport Management Company, `http://www.cyberport.com.hk/cyberport/en/home/home_flash.html`

[2] "u-Seoul," Seoul, `http://u.seoul.go.kr/` (in Korean)

[3] "Knowledge Capital Project," Knowledge Capital Management Corporation, `http://kita-yard.com/en/kc/index.html`

[4] "Cognition against social safety," Korean Statistical Information System, `http://www.kosis.kr/` (in Korean)

[5] "u-Safe Gangnam," Gangnam-gu office in Korea, `http://usafe.gangnam.go.kr/u-safe_01.html` (in Korean)

[6] "Assisted GPS," Wikipedia, `http://en.wikipedia.org/wiki/Assisted_GPS`

[7] K. Takata, J. Ma and B. O. Apduhan, "A Dangerous Location Aware System for Assisting Kids Safety Care," in 20th International Conference on Advanced Information Networking and Applications, Vol. 1., pp. 657-662, April 18-20, 2006.

[8] M. Gruteser and D. Grunwald, "Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis," Mobile Networks and Applications, vol. 10, no.3, pp. 315–325, 2003.

[9] P. Bahl and V.N. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in Proceedings of IEEE Infocom 2000, Tel Aviv, Israel, Vol.2, pp.775–784, March, 2000.

[10] G. V. Zàruba, M. Huber, F. A. Kamangar, and I. Chlamtac, "Indoor location tracking using RSSI readings from a single Wi-Fi access point," Wireless Networks, Vol. 13, No. 2, Springer Netherlands, pp. 221–235, April, 2007.