LETTER

Location-aware and privacy-preserving approach for child-care and safety in ubiquitous computing environment

Jangseong KIM[†], *Nonmember*, **Taeshik SHON**[††], *and* **Kwangjo KIM**[†], *Members*

SUMMARY In this paper, we establish our system model over the sensor network addressing contradictory issue caused by mutual authentication and privacy protection of an end-user. Based on the system model, we propose the protocol for a location-aware and privacy-preserving approach for child-care and safety over wireless sensor networks. Although we illustrate our protocol over the sensor network, our protocol can be operated over various networks (*e.g.*, WiFi and UWB) which can provide RSSI (Received Signal Strength Indication). Compared to previous work, our protocol can enhance the accuracy of location information, preserve privacy of an end-user, and give the capability of controlling the child-care and safety service to an end-user.

key words: *Privacy protection, location supporting protocol, ubiquitous, child-care*

1. Introduction

Recently, ubiquitous technologies such as RFID and sensor network are becoming a part of our living. One of typical examples is ubiquitous IT city called 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.

Compared to 10 years ago, 61.4% people in Korea realize that safety level changes to unsafe and 54.1% people expect that the safety level of our society becomes deteriorated in near future [4]. 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. Therefore, u-City can be one of the promising technologies to provide child-care service to its inhabitants. In Korea, mobile service providers such as SKT, KTF, and LGT provide their own child-care & safety service providing periodic report of a child's location to his/her parents and the subscriber of these services are continuously increasing. From now, we call this service as child-care & safety service. Then, we can define the service using four components such as end-user, service provider, device and location determination technique. 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]. When the end-user becomes a legitimate subscriber of a child-care & safety service, the user should store various private information (*i.e.*, his/her mobile phone number, living space, frequent visiting place and *etc*) to the service provider. Then, the 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 been occurred (or periodic reporting is required), the service provider sends a warning message (or reporting message) 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; 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 the security requirements from the residents of the u-City.

Child-care and safety service in u-City should provide *mutual authentication* and *privacy protection of an end-user*. Our protocol delegates a role of location determination to a kid's device so that the deployed sensor nodes do not require to authenticate the kid'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 computational overhead. More precisely, our protocol satisfies lightweightness as the kid'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.

2. Our protocol

In this section, we describe our system and protocol for child-care and safety service in detail. Before describing our protocol, we summarize our notations used throughout this paper in Table 1.

2.1 Our system model based on sensor network

We propose our system model based on sensor network where RSSI based on RF in sensor node [7] is employed

[†] The authors are with the Department of Information and Communications Engineering, KAIST, Korea. Contact email: jskim.withkals@kaist.ac.kr

[††] The author is with the Convergence Solution Team, DMC R&D Center, Samsung Electronics. Corresponding author

DOI: 10.1587/trans.E0.??.1

Table 1 Notation

$BS/MO/SN$	Base Station / Mobile Operator / Sink node
$Credential$	A ticket for authentication
$HS/KD/U$	Home server / Kid's device / End-user
n	A user's access frequency
LDT	Location Determination Technique
PK_A/SK_A	A public key of entity A / A private key of entity A
S	A set of selected numbers which length should be larger than $2n$
$m_1 \Vert m_2$	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
$E\{m, K_A\}$	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
$R^i_A, i = 1, 2, \cdots$	A series of nonce generated by entity A which is usually a 64-bit pseudo random number.

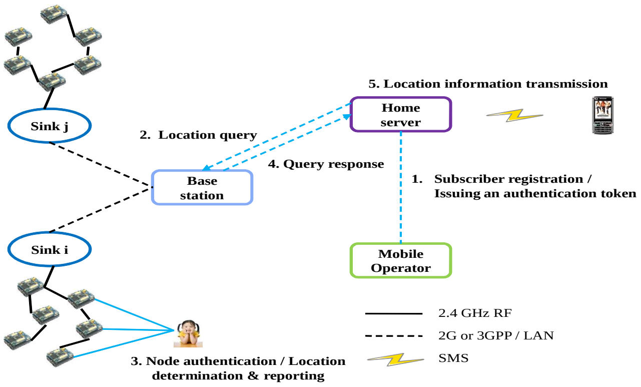
5. Location information transmission
Home server
Sink j
2. Location query
4. Query response
1. Subscriber registration / Issuing an authentication token
Base station
Sink i
Mobile Operator
3. Node authentication / Location determination & reporting
2.4 GHz RF
2G or 3GPP / LAN
SMS

Fig. 1 Our system model

to our location determination technique. We choose the sensor network to be our location determination technique due to the following observations. 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. When the location determination technique is changed to RSSI based on WiFi or UWB, our system model does not require any modification.

Fig. 1 shows our system model. In this model, a sensor network consists of sink nodes, sensor nodes, and a base station. A sensor node, having a battery power, gathers the nearby environmental information and sends the information to a sink node. Then, the sink node, having a permanent power and a capability of direct communication with the base station, aggregates the received information and forwards it to a base station. This approach can reduce unnecessary energy consumption of the intermediate nodes between a kid's device and base station, caused by forwarding authentication or service requests to the base station. As a result, our system model can increase lifetime of the sensor network. The base station verifies whether the end-user is one of legitimate subscribers or not. Only if the end-user is legitimate and registers location query of his/her kid, the base station stores the received authorized credential and kid's location, encrypted with a shared key between kid's device and end-user's home server, in its database.

Also, by increasing transmission power, a device of an end-user's kid can directly communicate with the sink node via another radio frequency, which is not used by the communication between a sensor node and sink node.

Finally, our system model includes a home server of an end-user to preserve the end-user's privacy as the system model proposed by Takata *et al.* [10]. 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. The home server periodically sends a query message including the registered credential in location query phase.

2.2 Our protocol for child-care and safety service

I our paper, we assume that an end-user can control the source addresses of the outgoing Medium Access Control (MAC) frames since it is a prerequisite for anonymous communications. Gruteser *et al.* [11] touched one of the detailed methods for this kind of modification but this is out of scope of this paper. Also, we assume that the base station consists of multiple servers in order to support the number of citizens in a city. To protect the base station from the numerous messages from the adversary, the base station should be kept through network security solution for DoS/DDoS attack. However, it is out of scope of this paper.

2.2.1 Subscriber registration

In subscriber registration phase, an end-user generates an authentication token and send the token to a mobile operator providing child-care and safety 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 for preserving an end-user's privacy, we adopt blind signature technique in [9] which provides enhanced security level, accountability, and non-linkability with less communications cost and computation cost. Based on our assumption and blind signature technique, the base station cannot distinguish two different end-users accessing the service. Also, the blind signature technique in [9] allows an end-user to obtain valid signature of the mobile operator while hiding the relation between the end-user's identity and obtained signature.

2.2.2 Location query

In location query phase, the end-user registers his/her au-

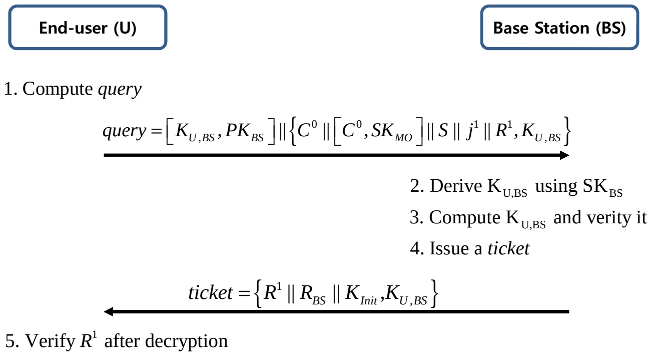
End-user (U)
Base Station (BS)
1. Compute *query*
$query = [K_{U,BS}, PK_{BS}] \| \{C^0 \| [C^0, SK_{MO}] \| S \| j^1 \| R^1, K_{U,BS}\}$
2. Derive K_{U,BS} using SK_{BS}
3. Compute K_{U,BS} and verity it
4. Issue a *ticket*
$ticket = \{R^1 \| R_{BS} \| K_{Init}, K_{U,BS}\}$
5. Verify R^1 after decryption

Fig. 2 Location query phase

thorized token with the base station. In addition, the end-user can control child-care and safety service by registering or deregistering his/her token to the base station. This approach can remove the end-user's concern about illegal tracking by the mobile operator or base station. Figure 2 depicts this phase.

2.2.3 Device authentication

Device authentication is required to share a fresh session key between kid's device and its nearby sink node. The session key can prevent an adversary from minimizing lifetime of the sensor network by sending unauthorized authentication requests. Since the kid's device sends an authorized token, the base station only recognizes that one of legitimate subscribers owns the device.

2.2.4 Location determination

Using triangulation based on RSSI [7] from three or more legitimate sensor nodes, the device can determine its location within 3 meters. As our interest is not 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 $R_{SN} \| C^{i-1} \| E\{ZONE \| R_{KD} \| R_{BS}, K_{HS,KD}\}$ with its HMAC to its nearby sink nodes.

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

After the base station received the message, the base station verifies integrity of the received 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 $E\{ZONE \| R_{KD} \| R_{BS}, K_{HS,KD}\}$ in its database. Otherwise, the base station drops the received message. Figure 3 illustrates this procedure.

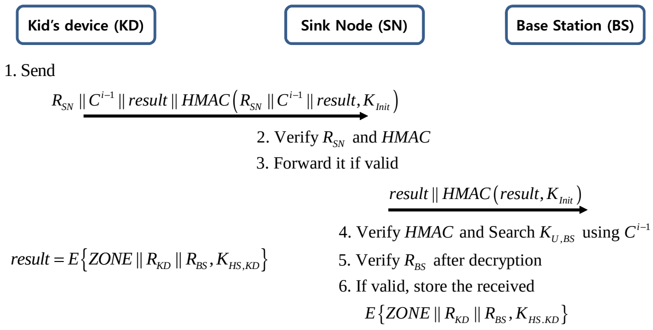
Kid's device (KD)
Sink Node (SN)
Base Station (BS)
1. Send
$R_{SN} \| C^{i-1} \| result \| HMAC(R_{SN} \| C^{i-1} \| result, K_{Init})$
2. Verify R_{SN} and *HMAC*
3. Forward it if valid
$result \| HMAC(result, K_{Init})$
$result = E\{ZONE \| R_{KD} \| R_{BS}, K_{HS,KD}\}$
4. Verify *HMAC* and Search $K_{U,BS}$ using C^{i-1}
5. Verify R_{BS} after decryption
6. If valid, store the received
$E\{ZONE \| R_{KD} \| R_{BS}, K_{HS,KD}\}$

Fig. 3 Location determination phase

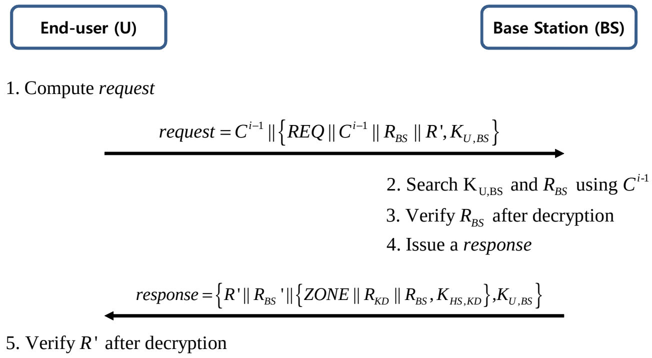
End-user (U)
Base Station (BS)
1. Compute *request*
$request = C^{i-1} \| \{REQ \| C^{i-1} \| R_{BS} \| R', K_{U,BS}\}$
2. Search K_{U,BS} and R_{BS} using C^{i-1}
3. Verify R_{BS} after decryption
4. Issue a *response*
$response = \{R' \| R_{BS}' \| \{ZONE \| R_{KD} \| R_{BS}, K_{HS,KD}\}, K_{U,BS}\}$
5. Verify R' after decryption

Fig. 4 Query response phase

2.2.5 Query response

In query response phase, an end-user sends a location request to the base station via his/her home server. 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 same credential stored in its database. Note that location information of the end-user's kid is encrypted with the shared key between a home server and kid's device. Figure 4 shows query response phase.

2.2.6 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.

3. Analysis

Since the existing approaches are based on A-GPS, the performance comparison between our protocol and the previous approaches is not meaningful. That's why we only show the properties comparison in Table 2. The existing services in Korea employs Assisted GPS to determine an end-user's location whether the end-user exists indoor or outdoor. Although the services have 10m accuracy in outdoor environ-

Table 2 Properties comparison of the previous work with our protocol

Properties	Existing services in Korea	Takada *et al.* [10]	Ours
Role of risk analysis	Service provider	End-user	End-user
LDT	A-GPS	A-GPS	RSSI based on RF
Accuracy in indoor Accuracy in outdoor	∼ 2km ∼ 10m	∼ 2km ∼ 10m	∼ 3m ∼ 3m
Supporting area	Outdoor & Indoor	Outdoor & Indoor	Indoor & outdoor†
Cost	High	High	Medium
Communication	Direct	Indirect	Direct
Infrastructure for location reporting	O	X	O
End-user Privacy	X	O	O
Controllability of an end-user	X	O	O

† : An area supporting RF communication

Table 3 Computational overhead in each phase

Phases	Entity	Public key Enc. / Dec.	Symmetric key Enc. / Dec.	Hash Operation
LQ	U	1(off-line)	1	1
	BS	1	1	1
LD	KD	0	1	2
	SN	0	0	2
	BS	0	0	2
LR	U	0	3	0
	BS	0	2	2

LQ : Location query *LD* : Location determination
LR : Location response

ment, accuracy of the services is changed to 2km in indoor environment. Since the signal strength of GPS is too weak for location determination in indoor environment, accuracy of GPS does not influence accuracy of the service in an indoor environment.

In our protocol, a child's device only requires RF communication module (or WiFi module) while the device in the previous work should include A-GPS and any communication module (*e.g.*, 3G network and WiFi). Compared to the device cost in the previous work, the device with WiFi or RF module in our protocol is 2 or 20 times more inexpensive, respectively. As the number of the service subscribers increases, the device cost for the service subscribers will increase linearly. Although our protocol requires the infrastructures such as wireless sensor network or WiFi network, this deployment cost is relatively smaller than the reduced device cost for the service subscribers. From this point, we believe that our approach is useful in u-City, which is a typical example of ubiquitous computing environments.

By deploying several access points (*e.g.*, sink node in our protocol), our protocol can provide the child-care & safety service in outdoor environment. Also, in u-City, these access points may be deployed to support seamless connection for the subscribers.

Computational cost We present computational cost of each phase in Table 3. If an "off-line" term exists, the computation can be done prior to the session. Since a kid'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 ubiquitous computing environment.

4. Conclusion

In this paper, we propose a location-aware and privacy-preserving approach for child-care and safety in ubiquitous computing environment. Our main contribution is to preserve privacy of an end-user while enhancing the accuracy of the child location to 3 meters. 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 WiFi RSSI and UWB RSSI can be applied to our protocol without any modification if the device of the target child supports Wi-Fi and UWB. By restricting a role of child-care & safety service provider to issue an authorized credential for an end-user's anonymity, the end-user can preserve his/her private information. Whenever the user wants the child-care and safety service, the end-user can register and deregister the service.

References

[1] Cyberport Home Page, `http://www.cyberport.com.hk/cyberport/en/home/home_flash.html` (accessed 12/17/09).

[2] u-Seoul Home Page, `http://u.seoul.go.kr/` (accessed 12/17/09), written in Korean.

[3] Knowledge Capital Project Home Page, `http://kita-yard.com/en/kc/index.html` (accessed 12/17/09).

[4] Cognition against social safety, 2008 database, `http://www.kosis.kr/` (accessed 12/17/09), written in Korean.

[5] Assisted GPS, Wikipedia, `http://en.wikipedia.org/wiki/Assisted_GPS` (accessed 12/17/09).

[6] N. Priyantha, A. Chakraborty and 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 and 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 and I. Chlamtac, "Indoor location tracking using RSSI readings from a single Wi-Fi access point", *Wireless Netw*, 2007, 13, 221–235.

[9] J. Kim, Z. Kim and 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.

[10] 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*, Vienna, Austria, April 18-20, 2006; pp. 657–662.

[11] 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.