Certification of Secure Encounter History Among Low Power Mobile Sensors

Takurou Sakai, Akira Uchiyama, Yoshitaka Nakamura and Teruo Higashino

Abstract In this paper, we propose a technique for certifying encounter information with acquaintances in wireless sensor networks. In our technique, we assume that each user holds a small low power sensor with a short range wireless communication device such as ZigBee, and that multiple sensors called landmarks, which provide accurate location and time, are sparsely distributed in the target area. Each user's sensor stores encounter information obtained from other users and landmarks in its memory, and it sends those information to its local server when it meets with landmarks which are connected to the Internet. At the same time, we assume that each user registers his/her private key and the list (called friend list) of his/her acquaintances in the Certification Authority (CA) server. When each user sends his/her encounter information to CA, CA informs the digital evidence about when and whom each user has met. In order to keep privacy of each encountered person, if an encountered person does not register the user's name in his/her friend list, the user cannot know that the user has met with the encountered person. Thus, our technique guarantees anonymity and unlinkability of encounter information by using a hash function and symmetric-key encryption. We have implemented the proposed technique using a hash function SHA-1 on MOTE and confirmed efficiency of the proposed technique through experiments. In addition, we have theoretically analyzed its low energy consumption and practical ability about traceability.

Takurou Sakai, Akira Uchiyama and Teruo Higashino
Graduate School of Information Science and Technology, Osaka University, 1-5 Yamadaoka, Suita, Osaka 565-0871, Japan, e-mail: {t-sakai,utiyama,higashino}@ist.osaka-u.ac.jp

Yoshitaka Nakamura
Graduate School of Information Science, Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma, Nara 630-0192, Japan, e-mail: y-nakamr@is.naist.jp

1 Introduction

As the progress of wireless network, it has been easy for a user to acquire information about the location. Therefore, many location-aware services such as E-911 [1] have been proposed. These services provide each user's location information about where the user is standing and give guides to the destination of the user. However, it is helpful for location-aware services to provide not only such location information but also encounter information which informs whom the user encounters at each time. In addition, if we can obtain the digital evidence of these information, we can provide several types of new location-aware services based on users' traceability.

For example, in Japan, most children go to their school on foot. Therefore we need a system to guarantee children's security by checking the behavior of the children on the way between the school and their home. When a child leaves from his/her school district, the system reports warning messages to his/her parents by using encounter information between the child and the terminals that the school deployed, and/or other children, teachers and inhabitants hold.

Ref. [2] proposes a routing protocol using encounter information. In Ref. [3], a search and rescue system called CenWits is proposed. In CenWits, each user holds a small sensor with a short range wireless communication device. Each user obtains and stores encounter information if he/she encounters other users or fixed base stations, which provide their own accurate location and time. Each user sends accumulated encounter information to a central server via base stations. The server estimates those users' location based on the accumulated encounter information. However, malicious users such as stalkers can easily track their favorite users' behavior since all messages are exchanged without encryption in CenWits. Additionally, malicious users might forge false encounter information. On the other hand, various techniques to certify users' location have been proposed so far [4, 5, 6, 7, 8]. Ref. [4] proposes a location certification technique called SECTOR, which certifies the correctness of users' location by using contact information with others. Most of location certification techniques use the distance bounding protocol [9] in which a node estimates the upper bounds of distance to another node by measuring communication delay. In the distance bounding protocol, special devices are assumed to measure time delay between nodes in nanoseconds.

In this paper, we propose a certification technique for encounter information which has (i) anonymity (i.e., no one can identify users only from encounter information), (ii) unlinkability (i.e., no one can recognize whether senders of multiple encounter information are the same or not) and (iii) digital evidence (i.e., malicious users cannot falsify encounter information). Hereafter, if encounter information satisfies unlinkability, we call it *unlinkable*, otherwise we call it *linkable*.

In order to keep anonymity, senders in encounter information should not be identified so that any user cannot identify them. Even if encounter information is anonymous, it might be linkable. For example, assume that encrypted encounter information sent from user i at time t_1 and t_2. If the identification of user i is encrypted as "111" and t_1 and t_2 are encrypted as "10001" and "10010", respectively, and if those two encounter information are simply specified as "<111,10001>" and

"<111,10010>", then others can identify these encounter information are sent from the same user "111" although they cannot identify the real user name of "111". If someone watches the user *i* transmits encounter information "<111,10001>", he/she can recognize the user of "111" is *i* when he/she meets user *i* again. Therefore, we need to design unlinkable encounter information. For digital evidence of encounter information, we need a trustful authority, that is, *Certification Authority* (CA) which certifies encountered location and time. In addition, CA needs to confirm encounter information is not falsified.

Generally, digital signature [10] using public-key encryption is used for authentication. There are many public-key encryption algorithms such as RSA [11], Elliptic Curve Cryptosystem (ECC [12]) and NTRU [13]. Although NTRU is lower cost algorithm than RSA and ECC, Refs. [14, 15] show that computational cost of NTRU is the greatest in the three encryption algorithms (NTRU, AES [16] and SHA-1 [17]). To satisfy various demands (for example, users' demand may be that they can use terminals for a long time without energy charge, while system providers' demand may be that they make an application which less influences other functions on mobile phones.), we need to choose a low cost encryption algorithm as we can. Also, since public-key encryption is hard to manage many private keys and public keys, it is not suitable for our technique. Therefore, our technique uses Hashed Message Authentication Code (HMAC [18]) and symmetric-key encryption (e.g., AES) to achieve anonymity and digital evidence. HMAC is one of message authentication techniques using a hash function with private keys. It achieves authentication and detection of falsification. In addition, we use randomized numbers in our technique to achieve unlinkability [19, 20].

We have evaluated our technique theoretically and chosen the hash function SHA-1 [17] on MICAz MOTE to evaluate computational time and energy consumption. Our theoretical analysis shows our technique is able to track users in urban areas with enough accuracy. From the experimental results on MOTE, we have confirmed that the execution time to compute SHA-1 for input size 1024 bits is 64 ms. Also, we have found that the energy consumption of SHA-1 is approximately 1/270 of RSA-1024 [21].

2 Overview

2.1 System Model

In our technique, we assume that base stations which provide accurate location information to users are sparsely distributed in the target area. Hereafter, we call those base stations *landmarks*. Some landmarks are connected to the Internet and forward encounter information sent from each user to *Local Server* (LS) of the user. Each user holds a mobile phone or a small low power sensor with a short range wireless communication device such as ZigBee and Bluetooth.

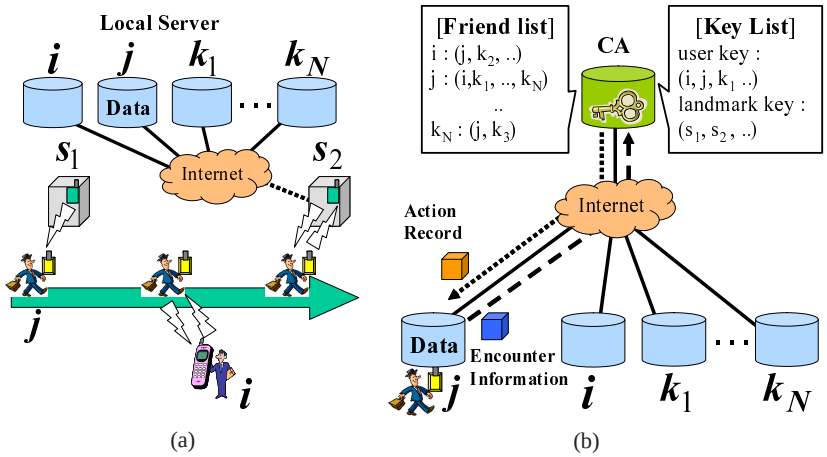

Fig. 1 System Model - (a) Gathering Encounter Information, (b) Certification Process

Each node periodically broadcasts beacon messages to its neighbors. When node j located in node i's wireless communication range receives i's beacon, j replies to i in order to confirm that i and j have encountered. Then j stores encounter information which certifies that i has encountered j (Fig. 1(a)). All exchanged messages are encrypted to avoid eavesdropping. Accumulated encounter information are forwarded to the user's LS when each user encounters landmarks.

CA certifies encounter information of each user if needed. From encounter information stored in LS of j, CA identifies the nodes which have encountered j, and certifies digital evidence of j's encounter information (Fig. 1(b)). Each user specifies *friends* in its own *friend list* in advance, and all friend lists are registered in CA. CA certifies encounter information if and only if i is a friend of j. Otherwise, CA discards encounter information. The certified encounter information is sent back to j as an action record of j, and j can show the persons that j has encountered and their encountered location and time with digital evidence.

2.2 Applications

Our technique assumes that it is used for the following applications.

- Children Security System
  In Japan, most children go to the school on foot along the pre-specified school roads (recommended safe routes to the school). Therefore we can check the security of each child if we can detect that the child moves along his/her school road or the child is in the school district. For this system, the school installs landmark terminals all over the school district, and children, teachers, inhabitants shall

have handheld unit with GPS function. When each terminal meets with other terminals, the system records its encounter information. Using this encounter information, when a child leaves from his/her school district, the system can detect the situation and notify the warning to parents of the child. And in case that a child does not come back home, if parents acquire this encounter information, they can acquire the information about where is the child and whom there is the child with now.

- Stray Child Discovery System
  The visitors of amusement parks are mainly families. There are many stray children in a park because they can walk freely. The users can enjoy the amusement park if they can find the lost child easily. The amusement park sets up a landmark terminal for each attraction, and each employee of the park carries a handheld terminal with GPS function. And the user of the park has a sensor terminal at the time of entrance. When the user meets with an employee or passes the neighborhood of the attraction, the user can acquire his/her correct location. In addition, if a child has been outside of the park as a lost child, we can detect the situation immediately by setting the landmarks in the surroundings of the park. This system can be used in the various places such as ball parks or museums and so on, with the same purpose.

3 Encounter Certification Mechanism

In this section, we describe the encounter certification mechanism of our technique. We prove that encounter information has anonymity, unlinkability and digital evidence.

3.1 Assumptions

Landmarks are given correct location coordinates. We assume that users have terminals with GPS function. We also assume loose time synchronization in all the terminals. In other words, they can obtain correct location and time. Let node i's location and time be l_i and t_i, respectively. In addition, we do not assume the multi-hop communication of nodes. These assumptions are relaxed in Section 3.3.

CA (Certificate Authority) does not hold encounter information itself but it keeps each user's identification, private key and friend list, which is the list of partners permitting to share the information about the user. Encounter information is stored in LS (Local Server) of the user and transmitted to CA only when the user needs certification. CA specifies the terminal (other user or a landmark) which the user met with from the encounter information and friend list of the user.

Each node encodes its sending data by using HMAC and AES to achieve anonymity. $H[text]$ and $mac_i(text)$ denote the output of hash function and HMAC

of text, respectively. We assume only CA and node i know i's private key. Since $mac_i(text)$ is generated by i's private key and $text$, CA can certify that the generator of $mac_i(text)$ is i. The encrypted data of $text$ is denoted as $aes_i(text)$.

A random number, which is changed every period of time, is input to HMAC together with sending data [19, 20]. This random number makes the sending data unlinkable since other users can only recognize it as a random bit sequence. We assume that this random number is created by a pseudo-random number generator (e.g., MD5 or SHA-1). Hereafter, r_i denotes a random number of node i.

3.2 Protocol

Node i is a supplier who provides encounter information. Landmarks and users can be node i. Node j is a claimant who receives encounter information, that is, only users can be node j.

1. Node i periodically broadcasts a beacon $beacon_{(i,t_i)} = \{h_i, c_i\}$.

$$h_i = mac_i(l_i, t_i, r_i)$$
$$c_i = aes_i(l_i, t_i, r_i),$$

   where l_i, t_i and r_i denote node i's location, time and random number, respectively.
2. Node j acquires encounter information $\{E_{ij}, < l_i, t_j >\}$ when j meets (i.e., received a beacon from) i as shown in Fig. 2.
   - Node j broadcasts $\{beacon_{(i,t_i)}, h_j\}$ and stores c_j.

$$h_j = mac_j(beacon_{(i,t_i)}, l_j, t_j, r_j)$$
$$c_j = aes_j(l_j, t_j, r_j),$$

     where l_j, t_j and r_j denotes node j's location, time and random number, respectively.
   - Node i broadcasts $\{h_j, h'_i, r'_i\}$ only if it receives $\{beacon_{(i,t_i)}, h_j\}$ in the time period of $[t_i, t_i + \Delta t]$.

$$h'_i = mac_i(h_j, r'_i),$$

     where r'_i denotes node i's random number.
   - Node j stores $\{E_{ij}, < l_i, t_j >\}$ only if it receives $\{h_j, h'_i, r'_i\}$ in the time period of $[t_j, t_j + \Delta t]$.

$$E_{ij} = \{beacon_{(i,t_i)}, h_j, h'_i, c_j, r'_i\}$$

3. Node j transmits $\{E_{ij}, < l_i, t_j >\}$ into its own LS via landmarks connected to the Internet.
4. Node j sends E_{ij} from its LS to CA for guarantee of its action record.

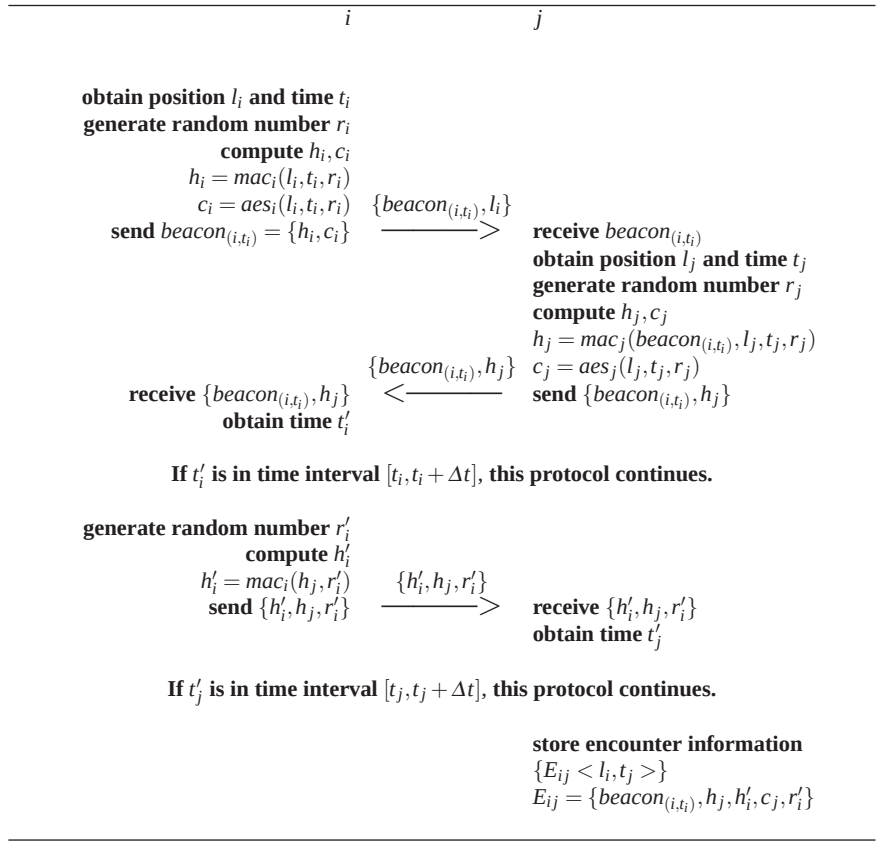

Fig. 2 Encounter Information Gathering Protocol

5. CA verifies E_{ij}.
   - CA specifies a node who node j encountered from h'_i.
     CA calculates $mac_k(h_j, r'_i)$ for all k in j's friend list, and compares it with h'_i.
     If they are corresponding, j encountered with k and h_j is not falsified.
   - CA specifies node j's location and time from h_j
     CA obtains $\{l_j, t_j, r_j\}$ by decoding c_j. CA calculates $mac_j(beacon_{(i,t_i)}, l_j, t_j, r_j)$ and compares it with h_j. If they are corresponding, l_j, t_j and h_i are not falsified.
   - CA specifies node i's location and time from h_i
     CA obtains $\{l_i, t_i, r_i\}$ by decoding c_i. CA calculates $mac_i(l_i, t_i, r_i)$ and compares it with h_i. If they are corresponding, l_i and t_i are not falsified.
   - CA guarantees encounter location l_{ij} based on l_i and l_j and encounter time t_{ij} based on t_i and t_j.
6. CA notifies the guaranteed encounter information $< i, l_{ij}, t_{ij} >$ to j.

3.2.1 Anonymity and Unlinkability

In this section, we prove anonymity and unlinkability of encounter information.

Lemma 1. *If text is changed at random every time,* $\{h_x, text\}$ *has anonymity and unlinkability, where* $h_x = mac_x(text)$.

Proof. Because $h_x = mac_x(text)$ can be generated only by a node which knows both x's private key and *text* according to the property of hash functions, only CA and x can identify x's private key from $\{h_x, text\}$. Therefore, $\{h_x, text\}$ has anonymity.

Additionally, if each sending data is changed at random every time, it is unlinkable. Assuming that *text* is changed at random every time, h_x becomes a random bit sequence since it includes *text* as input. Thus, $\{h_x, text\}$ is changed at random every time. Therefore, $\{h_x, text\}$ has unlinkability. □

Theorem 1. E_{ij} *has anonymity and unlinkability.*

Proof. We can consider E_{ij} to be consisted of $\lambda_1 = \{h_j, \{beacon_{(i,t_i)}, c_j\}\}$ and $\lambda_2 = \{h'_i, \{h_j, r'_i\}\}$. $beacon_{(i,t_i)}$, c_j and h_j are random bit sequences since those data include random numbers which are changed every time. In other words, $\{beacon_{(i,t_i)}, c_j\}$ and $\{h_j, r'_i\}$ are changed at random every time. Because the pair of λ_1 and λ_2 can be considered as $\{h_x, text\}$ in Lemma 1, E_{ij} has anonymity and unlinkability. □

3.2.2 Digital Evidence

We prove digital evidence of encounter information.

Theorem 2. E_{ij} *has digital evidence which shows that node i has encountered node j (i.e., it has existed within the wireless communication range of j) at time within* $[t_i, t_i + 2\Delta t]$.

Proof. Since only CA and i know i's private key, only i which knows h_j can generate h'_i, and since i generates h'_i only if it receives $\{beacon_{(i,t_i)}, c_j, h_j\}$ in the time period of $[t_i, t_i + \Delta t]$, h_j is generated within $[t_i, t_i + \Delta t]$. In other words, t_j is within $[t_i, t_i + \Delta t]$. In the same way, since only CA and j know j's private key, only j can generate h_j, and since j generates E_{ij} only if it receives $\{h_j, h'_i, r'_i\}$ in the time period of $[t_j, t_j + \Delta t]$, E_{ij} is generated in $[t_i, t_i + 2\Delta t]$. Therefore, E_{ij} has digital evidence which shows that i has communicated with j at time within $[t_i, t_i + 2\Delta t]$. Based on the assumption of multi-hop communication, i and j have existed in the wireless communication range of each other. □

Moreover, CA discards E_{ij} provided from nodes except node j.

Theorem 3. E_{ij} *is valid if and only if it is provided from node* j.

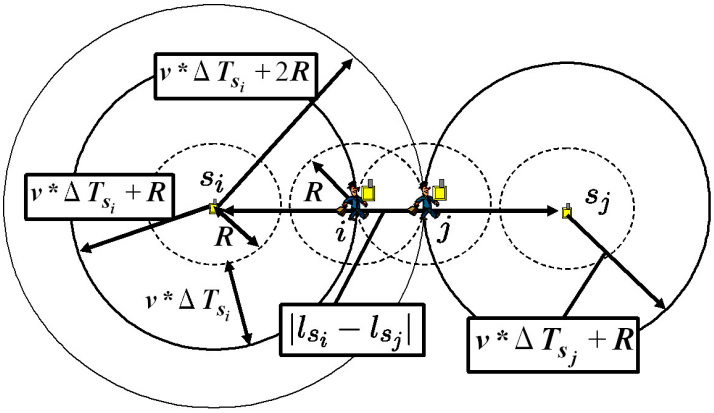

Fig. 3 Relation of Node Distances

Proof. CA finds that E_{ij} is encounter information involving node j since E_{ij} is provided from node j. Even though k provides E_{ij} to CA, CA can detect a contradiction as the following expression:

$$mac_k(beacon_{(i,t_i)}, l_j, t_j, r_j) \neq h_j$$

This is because node j's private key is unique. Therefore, E_{ij} is valid only for node j. □

3.3 Discussion

We relax the assumption of location, time and multi-hop communication.

3.3.1 Encounter Information Based on Landmarks

All users may not have GPS devices. Therefore, reliable information about location and time are provided from only landmarks. In such a case, our technique can estimate the region where the user has encountered the other node based on location of landmarks. Furthermore, our technique certifies the time sequence that the user encountered other nodes when the user does not have a timer device.

Encounter Region

If each user does not have a GPS device, reliable location information is obtained from only coordinates of landmarks. In this case, we assume that each node i pro-

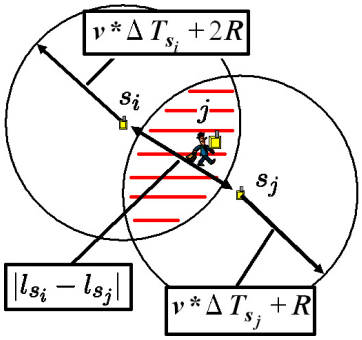

Fig. 4 Certified Encounter Region

vides substitutive information for its own location information l_i when i encounters other nodes. Each landmark s provides the pair of identifier id_s and location coordinate l_s. And each user i provides the pair of the location coordinate l_{s_i} of the last encountered landmark s_i and the elapsed time ΔT_{s_i} after the encounter with s_i. In addition, let the maximum velocity of users be v and the wireless communication range be R. In the following, v and R are common for all users to simplify the discussion, while different values can be set for each user. We also define $Circ(a,b)$ as a circular region whose central coordinate is a and radius is b. For example, we can express the region as $Circ(l_s,R)$ where the user can exist in wireless communication range R of the landmark s. Then CA certifies the following Theorem 4.

Theorem 4. *When users i and j encounter, the encounter location of j is in the following region.*

$$Circ(l_{s_i}, v*\Delta T_{s_i}+2R) \cap Circ(l_{s_j}, v*\Delta T_{s_j}+R) \tag{1}$$

Proof. Because j moves to distance of $v*\Delta T_{s_j}$ at the maximum when ΔT_{s_j} has passed since j encountered landmark s_j, j is in the region $Circ(l_{s_j}, v*\Delta T_{s_j}+R)$. i is also in the region $Circ(l_{s_i}, v*\Delta T_{s_i}+R)$. Therefore, since i and j are within the wireless communication range R of each other like Fig. 3, the location coordinate of j is certified to be in the common region of $Circ(l_{s_i}, v*\Delta T_{s_i}+2R)$ and $Circ(l_{s_j}, v*\Delta T_{s_j}+R)$ (Exp.1) as shown in the shaded region of Fig. 4. □

Time Sequence of Encounter

If each user does not have a timer device, reliable time information is only obtained from landmarks. In this case, we assume that each user i provides substitutive information for its own time t_i when i encounters other nodes. Each user i provides a hash value $H[E_{ki}]$ of encounter information E_{ki} with k which i has encountered last. If we assume that user j encountered $k_1, k_2, \cdots, k_n, i$ sequentially and k_1 is landmark s_j, then CA certifies the following Theorem 5.

Theorem 5. *E_{ij} certifies that node j encountered nodes $k_2, \cdots, k_n, i$ sequentially after the encounter with landmark s_j at t_{s_j}.*

Proof. E_{ij} includes the hash value $H[E_{k_n j}]$ of encounter information with k_n that node j has encountered last. Since node j cannot generate $H[E_{k_n j}]$ without $E_{k_n j}$, $H[E_{k_n j}]$ certifies that j encountered i at least after the encounter with k_n. The hash value $H[E_{k_{n-1} j}]$ of encounter information with k_{n-1} is also included in $E_{k_n j}$. Since we cannot generate $H[E_{k_{n-1} j}]$ without $E_{k_{n-1} j}$, $H[E_{k_{n-1} j}]$ certifies that j has encountered k_n at least after the encounter with k_{n-1}. In the same way, the hash value $H[E_{k_{n-2} j}]$ of encounter information with k_{n-2} is included in $E_{k_{n-1} j}$, and $H[E_{k_{n-2} j}]$ certifies that j has encountered k_{n-1} at least after the encounter with k_{n-2}. Therefore, $E_{k_n j}$ certifies that j has encountered k_{n-2}, k_{n-1}, k_n sequentially. When this procedure is repeated, $E_{k_n j}$ certifies that node j encountered nodes $k_1, k_2, \cdots, k_n$ sequentially. If we assume that the k_1 is the landmark s_j, $E_{k_1 j} = E_{s_j j}$ includes reliable encounter time t_{s_j}. Therefore, Theorem 5 is proved by deduction. □

3.3.2 Multi-Hop Communication

We assume that each node can communicate on multi-hop via other nodes. For example, if a malicious user simply installs a repeater between user i and user j, and the repeater sends the bit streams sent from i and j, it can fake as if i and j seems to have encountered. In other words, in Theorem 2, it is certified that i has communicated with j in $[t_i, t_i + 2\Delta t]$, but it cannot be certified that i and j has communicated directly. Therefore, it is necessary to certify that i and j are in the wireless communication range. In our technique, we can examine whether i and j are in each other's wireless communication range by location information provided from i and j.

However, i and j are assumed that they trust location information provided from each other (users do not give false evidence by location information). Because all users may not be reliable, we assume that a user can give false evidence for its location information. On this assumption, user j (or i) itself has to certify that the user i (or j) is in the wireless communication range, and has to store encounter information only when they are in the wireless communication range. This problem can be settled by using additional techniques such as the distance bounding protocol [9]. If we use the distance bounding protocol, a node can measure reliable distance with another node. However, the node needs a special device to measure accurate distance as described in Section 1.

It is also necessary to certify that the user possesses its own terminal. Our technique does not have means to certify whether the user possesses its own terminal. Therefore, our technique needs means that each user shows to possess its own terminal regularly. For example, each user has a terminal with a fingerprint authentication device or camera devices are sparsely distributed in the target area.

In this way, our technique can show reliable digital evidence of encounter information and certify anonymity at comparatively low cost. But using together with the existing techniques, our technique can show more reliable digital evidence of encounter information.

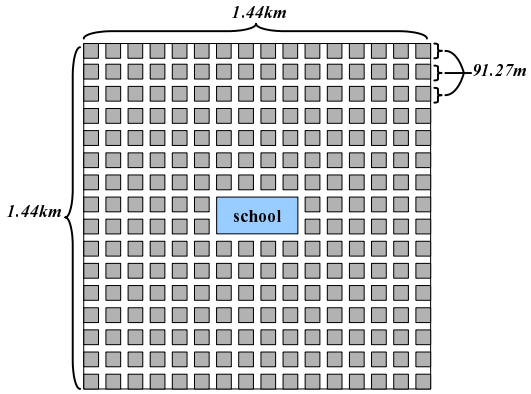

Fig. 5 A School District

4 Performance Evaluation

4.1 Traceability of Encounter Information

The number of landmarks to achieve traceability of encounter information differs depending on application requirements, that is, required frequency of obtaining encounter information. As an example application, we consider the children security system for primary students around Tokyo. For simplicity of discussion, we assume a square school district. In the city around Tokyo, the average size of a school district is $2.07km^2$ and the average length of a road is $91.27m$. Thus, the side of this square district is $1.44km$ by calculation of $2.07 = 1.44^2$ and the number of roads in the side is 16 from $1.44(km)/91.27(m) \simeq 16$. Therefore, we consider the application in the school district as shown in Fig. 5.

If we need to trace the movements of children at the road level in this whole district, encounter information is required on each road. Thus, we need to deploy $15^2 = 225$ landmarks at each intersection. On the other hand, we can reduce the number of landmarks in another requirement. Assume that the goal is detection of dangerous and/or abnormal movements of children. In Japan, most students go to the school on foot along the school roads (recommended safe routes to the school). Thus, we only need to deploy landmarks along with the school roads. In another requirement, we may want encounter information in every 5 minutes. Assuming that walking speed of children is $1.14(m/sec.)$, we need to deploy landmarks approximately every $340m(300(sec.) * 1.14(m/sec.))$. Thus, the required number of landmarks is 18 when considering the length of a road is $91m$. Moreover, students, teachers and inhabitants can be mobile nodes. In the $2.07km^2$ of the school district in this city, the average number of students, teachers and houses are 670, 30 and 4782, respectively. In addition, we may use base stations of wireless LAN in the houses as landmarks. Therefore, the number of landmarks can be reduced.

Table 1 Performance of MOTE

	MICAz	MICA2DOT
Processor	ATMega128L	
Clock Frequency	7.37 MHz	4 MHz
Program Memory	128 Kbytes	
SRAM	4 Kbytes	
Radio Frequency	2405 MHz	315/433/915 MHz
Bandwidth	250 Kbps	
Flash Memory	512 Kbytes	

4.2 Space Complexity

The data size of encounter information affects the number of information which a sensor can store in its memory. When node j obtains encounter information with node i, j stores $\{E_{ij}, < l_i, t_j >\}$ where $E_{ij} = \{beacon_{(i,t_i)}, h_j, h'_i, c_j, r'_i\}$. Since the beacon is $beacon_{(i,t_i)} = \{h_i, c_i\}$, E_{ij} consists of MAC values, codes of symmetric-key encryption and random numbers. MAC value is the output of the hash function. Here, we use the hash function SHA-256 [22] whose output size is 32 bytes. The size of random numbers can be small since quite different hash values are generated by a little change of random numbers. If a pseudo-random number generator is SHA-1, the size of random numbers is 20 bytes. Next, we consider the size of the codes. If we use AES as symmetric-key encryption, the output data size becomes multiple of block size of 16 bytes. When encounter information is certified based on information of landmarks, the input size of c_j becomes maximum. Then the input data of c_j is $(< l_{s_i}, \Delta T_{s_i} >, H[E_{k_n j}], r_j)$ instead of (l_i, t_i, r_i). Since l_{s_i} is x and y coordinates of a node, ΔT_{s_i} is the elapsed time, $H[E_{k_n j}]$ is a hash value and r_j is a random number, the data sizes of them are 6, 3, 32 and 20 bytes, respectively. Because at least 6 + 3 + 32 + 20 = 61 bytes are needed, we need to prepare 4 blocks (64 bytes) for the output of symmetric-key encryption.

Since the size of $beacon_{(i,t_i)}$ is $32 + 64 = 96$ bytes, we need $96 + 32 * 2 + 64 + 20 = 244$ bytes per E_{ij}. Therefore, we need $244 + 3 + 3 = 250$ per encounter information. If the memory capacity of a small sensor is 512 Kbytes as described in Table 1, the sensor can store $512 * 1000/250 = 2048$ encounter information. The time when the memory capacity is filled with the data changes with the interval of sending beacons and the nodes density. For example, assume that each node sends a beacon every 5s and each user encounters 10 nodes on average. Then, users can store encounter information on their small sensors for $2048/10 * 5 = 1024$s.

4.3 Computation Time

We have experimented to evaluate whether it is practical to implement the hash function on low power sensor nodes. We have used a small sensor MOTE which

Table 2 Energy Consumption of Three Encryption Algorithms on MOTE

Encryption Algorithm	Energy Consumption
RSA (RSA-1024)	304mWs
ECC (ECDSA-160)	22.82mWs
Hash Function(SHA-1)	5.9 μWs/byte

has a short range wireless communication device embedded with ZigBee called MICAz. Table 1 shows performance of MOTE. When we have implemented the hash functions SHA-1 and SHA-256 [22] on MOTE, we have found that it took 64ms and 170ms to compute each hash function for 1024 bits of input size. In our technique, the main process of sensors is computation of the hash function and the symmetric-key encryption. The computation time of the hash function is nearly equal to that of the symmetric-key encryption as described in Refs. [23, 24]. Therefore, encounter information can be generated within practical amount of time on a small low power sensor.

4.4 Energy Consumption

We compare the energy consumption of the hash function with that of public-key encryption. Refs. [23, 25] describe the energy consumption of RSA, ECC and the hash function implemented on MICA2DOT. The performance of MICA2DOT is described in Table 1. Table 2 shows the energy consumption of these three encryption algorithms.

We obtain the energy consumption of the hash function not for 1 byte but for the maximum input data size in our technique. When encounter information is certified based on information of landmarks, the input data of h_j becomes the maximum. Then the input data h_j is $(beacon_{(i,t_i)}, < l_{s_i}, \Delta T_{s_i} >, H[E_{k_n j}], r_j)$ instead of $(beacon_{(i,t_i)}, l_j, t_j, r_j)$. According to Section 4.2, each data size of $beacon_{(i,t_i)}$, l_{s_i}, ΔT_{s_i}, $H[E_{k_n j}]$ and r_j are 80, 6, 3, 32 and 20 bytes, respectively. So, the input data size of the hash function becomes 141 bytes at the maximum. Since the hash function is processed every block, we need to compensate an insufficient amount of multiple of block size. In other words, we need $64 * 3 = 192$ bytes when the block size is 64 bytes. Consequently, in our technique, the energy consumption of the hash function is 5.9 μWs/byte * 192bytes = 1133 μWs = 1.133 mWs. This is 1/268 and 1/20 times as much as the energy consumption of RSA-1024 and ECDSA-160.

Next, we consider the encryption algorithm called NTRU [13] for mobile phones. Ref. [14] shows the performance comparison of ECC, NTRU, AES and SHA-1 algorithms on a RFID tag (see Table 3). The energy consumption of NTRU is approximately 18 times as much as that in SHA-1 or AES. Therefore, SHA-1 and AES are suitable for our technique because their computation time and energy consumption are small.

Table 3 Performance Comparison of Four Encryption Algorithms on a RFID Tag

Encryption Algorithm	ClockCycle	Area(gates)	Energy(J)
ECC	408850	18720	322.5 μ
NTRU	29225	2850	1118.15 n
AES	534	4070	58.3 n
SHA-1	405	4362	50.35 n

5 Conclusion

In this paper, we have proposed a sensor-based certification technique for encounter information. In the proposed technique, users can obtain anonymous and unlinkable encounter information with digital evidence. We have implemented the hash function SHA-1 on MOTE to confirm whether it is possible to implement our technique on small low power sensors. We have found that the computation time of the hash function is short enough and its energy consumption is smaller than public-key encryption. For future work, we are planning to evaluate the performance of our technique on accuracy and scalability.

References

1. Federal Communications Commission. *911 Services*. —http://www.fcc.gov/911/enhanced/—.
2. M.Grossglauser and M.Vetterli. Locating Mobile Nodes with EASE: Learning Efficient Routes from Encounter Histories Alone. *IEEE/ACM Transactions on Networking*, 14(3):457–469, 2006.
3. J.Huang, S.Amjad, and S.Mishra. CenWits: A Sensor-Based Loosely Coupled Search and Rescue System using Witnesses. In *Proc. of ACM Conference on Embedded Networked Sensor Systems*, pages 180–191, 2005.
4. S.Capkun, L.Buttyan, and J.P.Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 21–32, 2003.
5. L.Lazos, S.Capkun, and R.Poovendran. ROPE: Robust Position Estimation in Wireless Sensor Networks. In *Proc. of Information Processing in Sensor Networks*, pages 324–331, 2005.
6. K.B.Rasmussen, S.Capkun, and M.Cagalj. SecNav: Secure Broadcast Localization and Time Synchronization in Wireless Networks. In *Proc. of ACM Conference on Mobile Computing and Networking*, 2007.
7. N.Sastry, U.Shankar, and D.Wagner. Secure Verification of Location Claims. In *Proc. of ACM Workshop on Wireless Security*, pages 1–10, 2003.
8. L.Lazos and R.Poovendran. SeRLoc: Robust Localization for Wireless Sensor Networks. *ACM Transactions on Sensor Networks*, 1(1):73–100, 2004.
9. S.Brands and D.Chaum. Distance-Bounding Protocols. In *Proc. of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, pages 344–359, 1994.
10. The Internet Society. *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, 2002.
11. R.L.Rivest, A.Shamir, and L.Adelman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

12. N.Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.
13. A.S.Wander, N.Gura, H.Eberle, V.Gupta, and S.C.Shantz. NTRU: A Ring-Based Public Key Cryptosystem. In *Proc. of the Third International Symposium on Algorithmic Number Theory*, pages 267–288, 1998.
14. Jens-Peter Kaps. Cryptography for Ultra-Low Power Devices. PhD Dissertation, Worcester Polytechnic Institute, 2006.
15. L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede. An Elliptic Curve Processor Suitable For RFID-Tags. Cryptology ePrint Archive, Report 2006/227, 2006. http://eprint.iacr.org/.
16. National Institute of Standards and Technology(NIST). Federal Information Processing Standards Publication 197, 2001.
17. D.Eastlake and P.Jones. US Secure Hash Algorithm 1 (SHA1). RFC3174, 2001.
18. R.Canetti M.Bellare and H.Krawczyk. Keying Hash Functions for Message Authentication. In *Proc. of Cryptology Conference on Advances in Cryptology*, pages 1–15, 1996.
19. S.A.Weis, S.E.Sarma, R.L.Rivest, and D.W.Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Proc. of Security in Pervasive Computing*, pages 201–212, 2004.
20. Y.Nohara, S.Inoue, K.Baba, and H.Yasuura. Quantitative Evaluation of Unlinkable ID Matching Schemes. In *Proc. of Workshop on Privacy in the Electronic Society*, pages 55–60, 2005.
21. C.K.Koc. High-Speed RSA Implementation. Technical report, RSA Laboratories, 1994.
22. National Institute of Standards and Technology(NIST). Federal Information Processing Standards Publication 180-2, 2004.
23. A.S.Wander, N.Gura, H.Eberle, V.Gupta, and S.C.Shantz. Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks. In *Proc. of IEEE Conference on Pervasive Computing and Communications*, pages 324–328, 2005.
24. S.Chang, S.Shieh, W.W.Lin, and C.Hsieh. An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks. In *Proc. of ACM Symposium on InformAtion, Computer and Communications Security*, pages 311–320, 2006.
25. K.Piotrowski, P.Langendoerfer, and S.Peter. How Public Key Cryptography Influences Wireless Sensor Node Lifetime. In *Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 169–176, 2006.