IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 8, 2018, accepted May 23, 2018, date of publication June 13, 2018, date of current version July 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2847030

A Real-Time, Automated and Privacy-Preserving Mobile Emergency-Medical-Service Network for Informing the Closest Rescuer to Rapidly Support Mobile-Emergency-Call Victims

SHIN-YAN CHIOU[1,2,3] AND ZHEN-YUAN LIAO[1]
[1]Department of Electrical Engineering, College of Engineering, Chang Gung University, TaoYuan 33302, Taiwan
[2]Department of Nuclear Medicine, Linkou Chang Gung Memorial Hospital, TaoYuan 33305, Taiwan
[3]Center for Biomedical Engineering, Chang Gung University, TaoYuan 33302, Taiwan

Corresponding author: Shin-Yan Chiou (ansel@mail.cgu.edu.tw)

This work was supported in part by the Ministry of Science and Technology under Grant MOST 104-2221-E-182-012 and in part by the CGMH Project under Grant BMRPB46.

ABSTRACT As populations age, there is a growing need for the establishment and staffing of care centers, but the supply of such facilities is not keeping pace with demand. Existing hospitals, care centers, and other institutions currently provide care for many physically disabled and elderly patients. For these patients to go outside in the fresh air, they must necessarily leave their designated care areas, but this poses a risk of falls and other accidents, which can be particularly challenging to prevent or respond to the given staffing limitations. Such incidents can cause further physical and mental deterioration. Many studies have sought to minimize rescue response times by first establishing the incident location before alerting staff to respond. However, this approach does not guarantee minimized response times. This paper proposes an approach to allow medical staff to quickly arrive at the scene of an accident with patients and staff using mobile devices to automatically alert a central server of their current locations. In response to an accident notification, the server immediately alerts medical staff in closest proximity to the incident to respond, with the staff devices providing clear directions to reach the patient in distress, thus minimizing response times. The proposed system can operate while maintaining security and patient information privacy, including the data integrity, anonymity, authentication, location confidentiality, location unforgeability, and resistance to asynchronous and tracking attacks, and is implemented on Android smart phones. The proposed system can be used in homes, hospitals, care centers, or any other venue offering long-term care. This proposal is the first such real-time and automated emergency rescue alert system to provide both information privacy and authentication.

INDEX TERMS Security, mobile, emergency call, emergency medical service, privacy.

I. INTRODUCTION

Hospitals care for many patients and elderly people who, due to mobility issues, are at risk of falls, and may require quick response in the event of an accident, thus raising the need for medical staff to immediately and accurately locate accident victims. Positioning technology offers significant advantages to this end.

Long-Term Care: Today, many countries seek to establish long-term care systems to provide quality, affordable and universal care for the elderly, allowing them to enjoy their old age in a familiar environment, while reducing the burden of such care on the family. The desired concentration of such long-term care centers entails a significant staffing challenge, and potential staff must be willing to undergo extensive professional training, thus many such facilities may be understaffed. Elderly and disabled patients are free to roam the premises in such centers, but are prone to falls and accidents from which they may be unable to recover without assistance. In understaffed facilities, such accidents may not be immediately noticed, thus delaying treatment, potentially with severe consequences.

Traditional Emergency System: To address this issue, hospitals have established panic button systems to summon medical staff. However, not all areas of a facility to which patients have access necessarily have panic buttons and, even when a panic button is nearby, someone other than the accident victim must be available to press it or help the victim.

Class of Emergency System: Bastos *et al.* [1] reviewed the literature on the use of indoor positioning technologies for emergency response since 2004. Aside from comparing technology use and practices, they also classified each approach according to response requirements. Glanzer [2] suggested that, in general, personal and emergency response use require different levels of location precision, and reviewed most existing positioning technologies, categorizing them as for personal or emergency response use. In general, emergency response systems can be divided into two different types. In the first type, the response target waits passively for rescue while in the second s/he actively seeks assistance. Additional systems are designed for use by rescuers.

Emergency Rescue System for Passive Targets: This type of system focuses on the rescue of passive targets, in which the victims typically stay in one place and continuously transmit their positioning information. For example, in responding to a fire, firefighters or EMTs (Emergency Medical Technicians) can use a building's positioning system to assess victim location, and thus head directly to the appropriate floor, ensuring efficient rescue operations, where EMTs may refer ambulance men, emergency responders, or emergency-service personnel. In 2015, Berbakov *et al.* [3] proposed using built-in smart phone sensors to achieve positioning through dead reckoning. The resulting information could then be uploaded to a database for emergency use. In 2016, Srinivasan *et al.* [4] proposed a new rescue system incorporating three roles: Smart Building, Community Cloud, and Emergency Service Provider. A Smart Building will regularly upload its occupant distribution and status information to the Community Cloud for access by Emergency Service Providers in the event of an emergency. In 2013, Do *et al.* [5] proposed using RFID to establish positioning for rescue facilitation and to guide civilians to safety in the event of an emergency. In 2014, Li *et al.* [6] proposed a method of positioning rescuers and accident victims with room-by-room precision, thus facilitating deployment of equipment and staff. Nie *et al.* [7] proposed using Zigbee to implement interior positioning, and used physiological indicators to monitor the health status of miners, providing critical data to surface workers responding to an underground emergency.

Emergency Rescue System for Active Targets: Active targets track their own positions and send their location information to rescuers in the event of an accident. For example, lost or injured hikers will locate themselves by GPS and then attempt to transmit this information to the outside world. In 2014, Kau and Chen [8] proposed using smartphone sensors to detect user falls. Once a fall is detected, the device uses GPS to determine the user's location, and Wi-Fi or wireless networks to call medical staff to respond. In 2004, Liutkauskas *et al.* [9] proposed an Emergency Call Service for use in a range of environments with various positioning precision requirements and reliability to meet rescue needs, and also compared existing positioning technologies in terms of suitability for use by rescue services.

Emergency Rescue System: This type of system is used exclusively by first responders. In 2011, Amanantiadis *et al.* [10] proposed a system which integrated sensors, digital imaging and RFID to determine positioning according to status weightings in a fuzzy inference system, thus offering rescuers a robust and highly sophisticated navigation system. In 2013, Hari *et al.* [11] proposed a system incorporating inertial sensors embedded in the rescuer's shoes, along with helmet-mounted cameras to help rescuer's quickly locate and navigate through disaster sites. In 2012, Moon *et al.* [12] proposed using AP and Wi-Fi to provide firefighters with accurate positioning data to enhance on-site safety. In 2013, the same team proposed a new method which applied SLAM, EKF and other methods to the distance between two firefighters within earshot to calculate their relative positioning, thus allowing one firefighter to use the other as a positioning landmark [13]. In 2012 Pascucci *et al.* [14] proposed a low-cost, easy-to-implement and high precision positioning system for rescue personnel. In 2011, Rantatkokko *et al.* [15] proposed a sensor system for use in military rescue missions. In 2013, Zhang *et al.* [16] proposed an indoor positioning method using inertial sensors which could be used by emergency responders. In 2011, Pascucci and Setola [17] proposed using RFID positioning technology to assist evacuation, and this approach can also be used by rescue personnel and robots. In 2013, Zhang *et al.* [18] noted that existing systems were mostly unsuitable for use in emergency situations, and proposed adopting UWB technologies to assist first responders in emergencies. In 2012, Guiliano *et al.* [19] proposed a set of positioning tools to conduct a range of tests to confirm RFID reliability and accuracy to meet the needs of emergency responders. In 2012, Zhou *et al.* [20] proposed a long-wave positioning method which, compared to Zigbee, Wi-Fi and other short-wave methods, offered improved penetration and farther reach. Data transfer can then be accomplished through 3G, Wi-Fi or other short-wave communications.

Secure Emergency System: All of the above-mentioned rescue systems entail the use of personal location information, which may be inadvertently leaked to third parties or attackers, thus compromising user privacy. In 2016, Ghafghazi *et al.* [21] proposed an attribute-based encryption and broadcast encryption, using encrypted texts of consistent size to provide constant pairs for decryption. In 2016, Zhu *et al.* [22] proposed an encrypted text method using a special spatial range query algorithm which can ensure user location information security at the server end. In 2016, Yu *et al.* [23] proposed a privacy-preserving based scheduling scheme for emergency response which can protect location and other sensitive data.

Wireless body area network: A wireless body area network (WBAN), which is proposed by Zimmerman [27], is a wireless network of wearable computing devices and uses wireless personal area network (WPAN) technology [28] to collects real-time biomedical data through many low power intelligent sensors, placed in or around the human body, and sends the data to a remote medical server through mobile devices, providing a remote and real-time monitoring [29–31]. The standard IEEE 802.15.6 describes security requirements and various security levels in WBANs, and recommends four elliptic curve-based security schemes. However, Toorani indicates those schemes lacks forward secrecy, and is vulnerable to an impersonation attack, a KCI attack, and an invalid-curve attack [32], [33]. To enhance security for WBANs, anonymous authentication (AA) schemes [29] have been studied to provide authentication, privacy preservation, confidentiality, integrity, and nonrepudiation based on a shared key. However, He *et al.* [29] point out that AA scheme is not secure for medical applications by an impersonation attack.

Paper Contribution: This article focuses on active rescue approaches for use in hospitals and rest homes caring for disabled patients and residents. Accidents in such environments may occur in isolation, with no one at hand to report or assist. In such instances, the proposed system uses smart phones to ensure that the nearest available medical personnel are alerted and guided to the victim to minimize response times. In addition, user and staff location information is protected, and the system provides security features such as anonymity and information integrity.

Paper Structure: This paper is divided into six sections. Section two reviews the relevant literature to explain and analyze the referenced schemes. Section three describes the proposed emergency system's contents and structures. Section four analyze the proposed of six emergency requirements and seven security requirements. Section five describes an actual implementation using Android phone and section six draws a conclusion.

II. RELATED WORKS

This section introduce Srinivasan *et al.* [4] scheme because, compared to other schemes, only the function of their scheme is partially similar to ours.

Fires, earthquakes and other disasters are typically complicated by lack of preparedness. While local communities and government agencies may regularly conduct disaster prevention exercises, judgment can fail quickly in the event of an actual emergency. This can cause rescuers to fail to take the most secure route, leading to further accidents and casualties.

In 2016, Srinivasan *et al.* [4] proposed a system for emergency response within buildings. The system architecture included three roles: Smart Building, Community Cloud and Emergency Service Provider, and covered all interactions between these roles during normal operations and during emergencies. They also proposed means of handling sensitive information within the system.

To enhance rescue effectiveness, medical and disaster relief personnel can use their system to first familiarize themselves with the building's structure and determine the location of rescue targets before entering. In addition, the system provides rescuers with rescue target medical history and mobility status, thus facilitating rescue planning and likelihood of successful rescue. This section reviews and discusses the scheme of Srinivasan *et al.* [4].

A. REVIEW OF SRINIVASAN et al.'S SCHEME

As shown in Fig. 1, Srinivasan *et al.* [4] system has three roles: Smart Building, Community Cloud and Emergency Service Provider. These three roles respectively collect data, store data and act on the data to perform rescue work. The operations for each role in emergency and non-emergency conditions are described as follows:

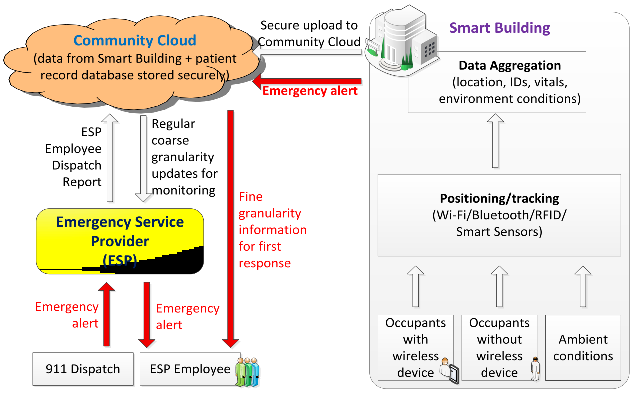

Community Cloud
(data from Smart Building + patient record database stored securely)
Secure upload to Community Cloud
Smart Building
Data Aggregation
(location, IDs, vitals, environment conditions)
Emergency alert
ESP Employee Dispatch Report
Regular coarse granularity updates for monitoring
Fine granularity information for first response
Positioning/tracking
(Wi-Fi/Bluetooth/RFID/ Smart Sensors)
Emergency Service Provider (ESP)
Emergency alert
Emergency alert
Occupants with wireless device
Occupants without wireless device
Ambient conditions
911 Dispatch
ESP Employee

FIGURE 1. Structure of Srinivasan *et al.*'s Emergency response system.

1) SMART BUILDING

A Smart Building is a structure equipped with multiple sensors. Our proposed method uses sensors to locate and track users, using technologies including RFID matrixes, Wi-Fi AP, Bluetooth Beacon, hand-held radars, etc. RFID matrixes can detect the movement of individuals in indoor environments, while hand-held radars can not only track human movement but can also detect the heart rate of individuals. People carrying mobile devices can be tracked through indoor positioning systems, which can also provide access to their corresponding medical history and records, thus allowing medical staff to better coordinate with rescuers.

Servers within the Smart Building can collect useful data from these sensors, including living conditions, occupancy distributions, and location and current trajectory of occupants. Through local area networks (LAN), this data can be uploaded to the Community Cloud, ensuring detailed data for the entire building is available to rescue workers in the event of an emergency.

2) COMMUNITY CLOUD

A Community Cloud is a cloud-based database which continually collects sensor data from a Smart Building, making this data easily available in the event of an emergency. Access restrictions are applied to provide different information granularity for scenarios.

In non-emergency situations, the Community Cloud provides rough resolution data to the Emergency Service Provider for use in monitoring building activities. However, in the event of an emergency, the Community Cloud can release detailed information to authorized medical staff, allowing for more efficient rescue operations.

3) EMERGENCY SERVICE PROVIDER

The Emergency Service Provider is a group which provides rescue services, including staff trained to provide medical services such as firefighters and other caregivers. In response to an alert, such as a building alarm being manually or automatically triggered in response to an emergency, the Emergency Service Provider immediately dispatches specialized medical staff to provide relief. These rescuers can then access real-time building information from the Community Cloud, to facilitate their rescue efforts.

B. PRIVACY CONCERNS

The information collected within a Smart Building is highly sensitive because the location of individuals within the structure can be actively and continuously tracked. The location and movement information of these individuals are stored in the Community Cloud, and can be released to the Emergency Service Provider and its medical staff members. Therefore, the transmission of this sensitive information poses a security risk. Location information is typically only stored for a minute or less, but leakage of these records to unauthorized users could pose a serious security risk to the building and its occupants.

In non-emergency situations, the Emergency Service Provider actively monitors the building status, for which it requires access to less-detailed data, thus the Community Cloud only provides low-granularity information that does not contain personal details, thus maintaining privacy. Also, such conditions do not require such a high degree of information density, and thus the Emergency Service Provider is only able to access building data once every 30 minutes to reduce the risk of building data from being behavior pattern analyzed.

When an emergency alert is raised, the Emergency Service Provider will send a medical staff team. The Community Cloud is already aware of the alert and thus authorizes the medical staff to access all building data, ensuring the team can operate with maximum effectiveness.

III. PROPOSED SCHEME

This section explains two proposed systems: (1) mobile emergency system (*MES*) and (2) secure mobile emergency system (*SMES*) with privacy and authentication.

A. MOBILE EMERGENCY SYSTEM (MES)

This section explains the system requirements and the detailed scheme of the proposed system

1) SYSTEM REQUIREMENT

System requirements of the proposed system are described as Definition 1.

Definition 1 (System Requirements): The proposed scheme should meet the following conditions. (1) provide real-time user location information, (2) immediately alert closest available medical workers, (3) provide medical staff with accurate real-time rescue location information, (4) provide server with continuous rescuer location updates, (5) ensure normal power consumption on user device (i.e., works in standby mode), (6) ensures user location information privacy (standby mode).

2) SCHEME OF MOBILE EMERGENCY SYSTEM

Based on Definition 1, we propose a new mobile emergency system (MES) which entails in two phases: normal-operation phase and emergency phase (Fig. 2).

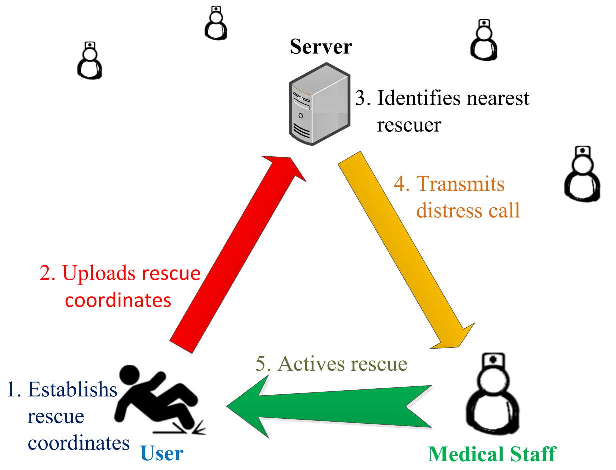

Server
3. Identifies nearest rescuer
4. Transmits distress call
2. Uploads rescue coordinates
5. Actives rescue
1. Establishs rescue coordinates
User
Medical Staff

FIGURE 2. Proposed mobile emergency system (*MES*).

a: NORMAL-OPERATION PHASE

During normal usage, only the server and medical staff are active in the system. Medical staff must continuously carry mobile devices which will regularly update their location information to the server. This data is stored in the Server's medical-staff-location database, which provides a real-time personnel location distribution for the entire building.

b: EMERGENCY PHASE

(1) *Establishing rescue coordinates:* When an accident victim in a hospital requires assistance, s/he can use a dedicated APP on her/his smart phone to send an alert. The APP simultaneously obtains the user's location information, and the user's coordinates are continuously updated until the incident is resolved.

(2) *Uploading rescue coordinates:* The user's smart phone uploads its current location information to the server,

allowing the server and medical staff to track the user's coordinates in real-time.

(3) *Identifying nearest rescuer:* The server searches its medical staff location database to identify the staff member closest to the person in need of assistance, ensuring prompt response.

(4) *Transmit distress call:* The server then sends a distress call to the mobile device of the medical staff member identified as being closest to the scene, accompanied by a map of the user's current location displayed on the staff member's mobile device. This audio/vibration alert serves as a continuous reminder that the staff member has been assigned a current urgent task.

(5) *Active rescue:* The charged medical staff member then follows the map and immediately proceeds to the scene to provide assistance.

3) COMMUNICATION PROTOCOL BETWEEN EACH ROLES

Our system entails three roles, medical staff, users and server. The communication methods are described as follows.

a: MEDICAL STAFF ONLINE

When a medical staff member is online, his/her mobile device first transmits his/her ID to the server for authentication. It then continuously updates his/her location information to the server every t sec. (e.g. 3 sec.) [26] (Fig. 3).

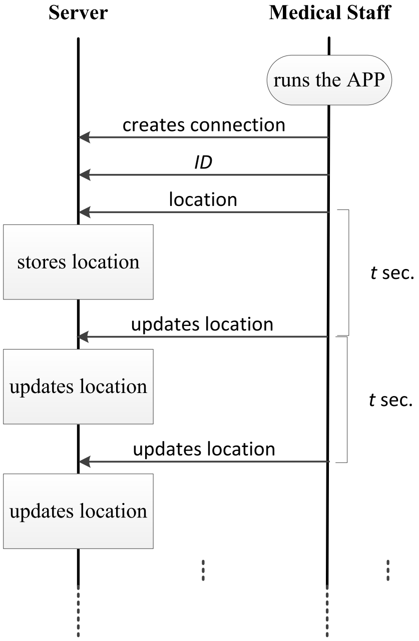


FIGURE 3. Medical staff online.

b: EMERGENCY OCCURRED

In the event of an emergency, the user's mobile device first sends an alert to the server (and continuously updates his/her alert and location information every t sec. (e.g. 3 sec.) [26]), which then immediately sends the rescue location information to all medical staff, and specifically calls the nearest available staff member to render assistance (Fig. 4).

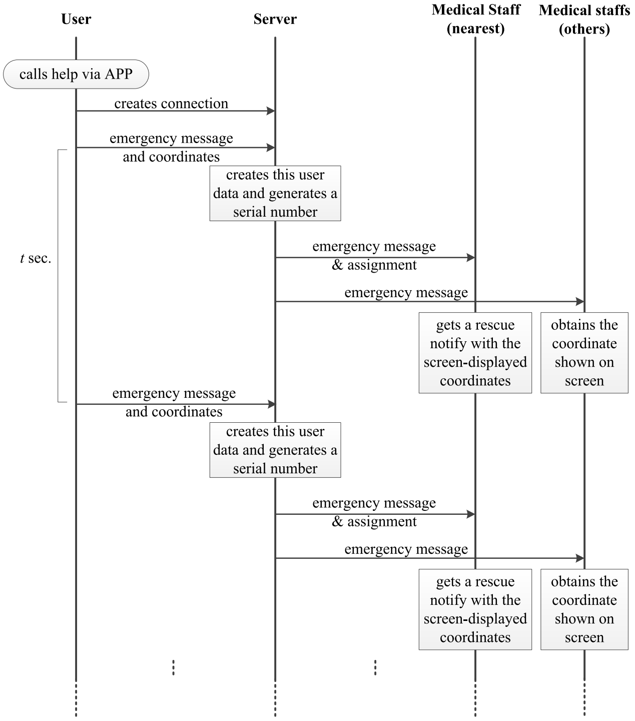

User
Server
Medical Staff (nearest)
Medical staffs (others)
calls help via APP
creates connection
emergency message and coordinates
t sec.
creates this user data and generates a serial number
emergency message & assignment
emergency message
gets a rescue notify with the screen-displayed coordinates
obtains the coordinate shown on screen
emergency message and coordinates
creates this user data and generates a serial number
emergency message & assignment
emergency message
gets a rescue notify with the screen-displayed coordinates
obtains the coordinate shown on screen

FIGURE 4. An emergency occurred.

c: CANCEL THE EMERGENCY

When the user can be assisted by others at the scene and does not require additional help, s/he can cancel the alert, causing the server to transmit a cancellation message to any alerted medical staff (Fig. 5).

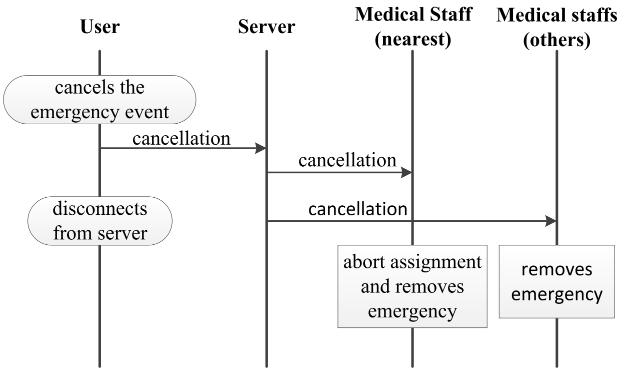


FIGURE 5. Cancel the emergency.

d: EMERGENCY HAS BEEN RESOLVED

When the alerted medical staff member has successfully assisted the user, s/he presses the "Solved" button in the APP, alerting other medical staff that the situation has been resolved. The user's mobile device will thus cease transmitting continuous location information to the server (Fig. 6).

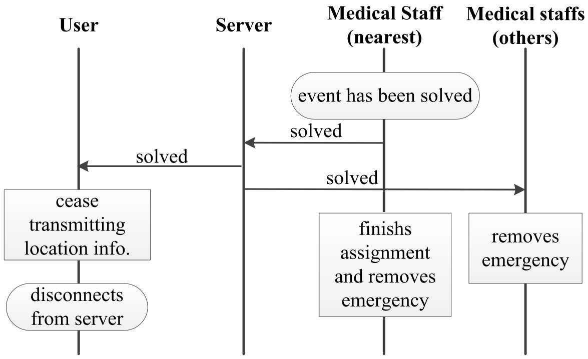


FIGURE 6. The emergency has been resolved.

B. SECURE MOBILE EMERGENCY SYSTEM (SMES)

The proposed *MES* can provide the requirements of mobile emergency system. However, there are many security issues such as location privacy and authentication. The proposed *SMES* can provide security requirements.

1) NOTATIONS

Our proposed secure mobile emergency system (*SMES*) contains three roles (User, Medical staff, and Server) and five phases (register phase, normal-operation phase, emergency phase, cancel phase, and resolved phase). Table 1 defines the symbols and parameters used in the proposed method.

TABLE 1. Notations.

Notation	Description
U / M / S	User / Medical Staff / Server
ID_X	the *ID* of *X*
SID_X	the pseudo *ID* of *X*
$BSID_X$	the backup pseudo *ID* of *X*
t_X	the extracted current time of *X*
T_{th_i}	the *i*-th time threshold
Loc	location information
DB	the database of stored location information
m_{ask}	a message to query whether medical staff accept to rescue
m_{accept} / m_{reject}	a message to response server whether medical staff accept to rescue
$m_{finding}$	a message that represent system is finding helpful medical staffs
m_{coming}	a message that represent medical staff is on the way to help
m_{cancel}	a message that represent user cancel this event
$m_{resolved}$	a message that represent medical staff has resolved this event
K_{AB}, K_{BA}	the shared key between *A* and *B*
$h(\cdot)$	one way hash function
$E_K(\cdot)/D_K(\cdot)$	symmetric encryption/decryption using key *K*

2) ATTACKER MODEL

In our scheme, any identity communicates with each other via an insecure public channel, offering adversaries opportunities to intercept. In the following, we present the assumptions of the attacker model.

(1) An adversary may eavesdrop on all communications between protocol actors over the public channel.

(2) An attacker can modify, delete, resend and reroute the eavesdropped message.

(3) An attacker cannot be a legitimate Server.

(4) The attacker knows the protocol description, which means the protocol is public.

3) SECURITY REQUIREMENT

The proposed secure mobile emergency system (*SMES*) ensures the privacy and authentication. Security requirements are described as Definition 2.

Definition 2 (Security Requirements): The proposed scheme should meet the following conditions.

(1) Data integrity: An attacker cannot alter the transmitted data without being detected.

(2) Anonymity: Aside from the server, the user's and medical staffs' identity should not be disclosed to anyone.

(3) Authentication: One of the legitimate roles (including server, users and medical staffs) should be able to proof of the identity of another.

(4) Location confidentiality: An attacker cannot disclose any location information.

(5) Location unforgeability: Aside from a legitimate users and medical staffs, no one should be able to successfully pose as one of these actors' location for authentication.

(6) Resistance to asynchronous attacks: Attackers should not be able to block data transmissions, causing the server, medical staffs or users to be unable to synchronously update, and thus undermining the following authentication iteration.

(7) Resistance to tracking attack: Attackers should not be unable to access information from the messages transmitted through the protocol to determine which users or medical staffs are involved a given communication session.

4) PROPOSED SECURE MOBILE EMERGENCY SYSTEM (SMES)

The proposed secure mobile emergency system (*SMES*) is based on both the system requirements in definition 1 and security requirements in definition 2. The proposed scheme entails five phases: registration phase, normal-operation phase, emergency phase, cancel phase, and resolved phase (Fig. 7).

a: REGISTRATION PHASE

In this phase, users and medical staffs proceed registration to the *Server*, allowing them to share a shared key K_{SA} and compute $SID_A \leftarrow h(ID_A, K_{SA}, 0)$, where $A = U$ or K (Fig. 8).

b: NORMAL-OPERATION PHASE

In this phase, medical staffs report their positions to the *Server* periodically, allowing the *Server*to build a real-time staff-location map instantly for the follow-up rescue. The detail steps are described as follows (Fig. 9).

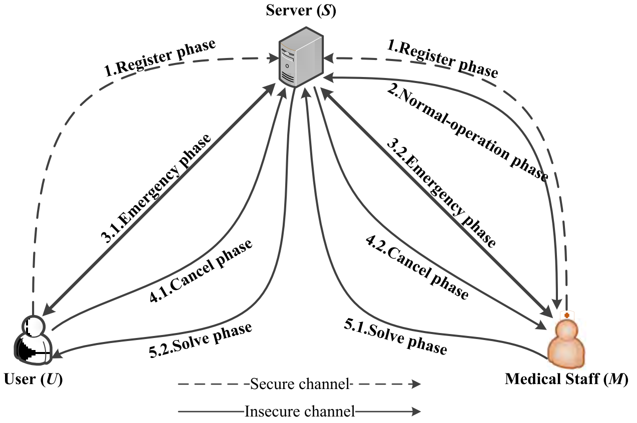


FIGURE 7. Proposed scheme of secure mobile emergency system (SMES).

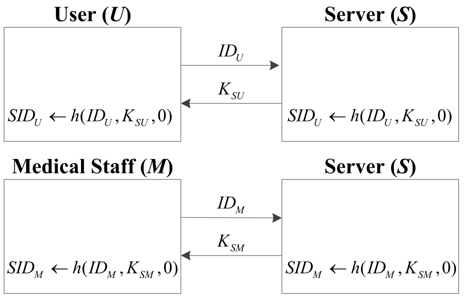
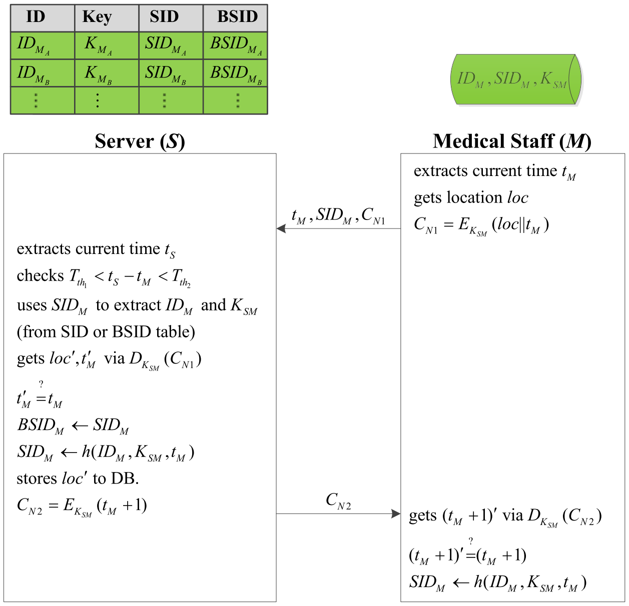

User (U)
Server (S)
ID_U
K_{SU}
$SID_U \leftarrow h(ID_U, K_{SU}, 0)$
$SID_U \leftarrow h(ID_U, K_{SU}, 0)$
Medical Staff (M)
Server (S)
ID_M
K_{SM}
$SID_M \leftarrow h(ID_M, K_{SM}, 0)$
$SID_M \leftarrow h(ID_M, K_{SM}, 0)$

FIGURE 8. Registration phase.



ID	Key	SID	BSID
ID_{M_A}	K_{M_A}	SID_{M_A}	$BSID_{M_A}$
ID_{M_B}	K_{M_B}	SID_{M_B}	$BSID_{M_B}$
⋮	⋮	⋮	⋮

ID_M, SID_M, K_{SM}
Server (S)
Medical Staff (M)
extracts current time t_M
gets location loc
$C_{N1} = E_{K_{SM}}(loc \| t_M)$
t_M, SID_M, C_{N1}
extracts current time t_S
checks $T_{th_1} < t_S - t_M < T_{th_2}$
uses SID_M to extract ID_M and K_{SM}
(from SID or BSID table)
gets loc', t'_M via $D_{K_{SM}}(C_{N1})$
$t'_M \overset{?}{=} t_M$
$BSID_M \leftarrow SID_M$
$SID_M \leftarrow h(ID_M, K_{SM}, t_M)$
stores loc' to DB.
$C_{N2} = E_{K_{SM}}(t_M + 1)$
C_{N2}
gets $(t_M + 1)'$ via $D_{K_{SM}}(C_{N2})$
$(t_M + 1)' \overset{?}{=} (t_M + 1)$
$SID_M \leftarrow h(ID_M, K_{SM}, t_M)$

FIGURE 9. Normal-operation phase.

(1) Medical staff extracts time t_M and location loc, uses the shared key K_{SM} to encrypt the message t_M and loc, and sends t_M, $E_{K_{SM}}(loc||t_M)$, SID_M to the *Server*.

(2) After the *Server* receives the message, it extracts time t_S and verifies whether $t_S - t_M$ is in the time interval (i.e. $T_{th_1} < t_S - t_M < T_{th_2}$). If it does, the *Server* uses SID_M to find ID_M and K_{SM}. If SID_M cannot be found from *SID* Table, the *Server* uses *BSID* Table to find them again. Next, it uses K_{SM} to decrypt $E_{K_{SM}}(loc||t_M)$ to obtain loc' and t'_M and verifies whether $t'_M \overset{?}{=} t_M$ hold. If it does, which means the *Server* authenticate the medical staff successfully, the *Server* updates *SID* Table and *BSID* Table, stores loc' in *DB*, and computes $E_{K_{SM}}(t_M + 1)$ and sends it to medical staff.

(3) The medical staff uses K_{SM} to decrypt $E_{K_{SM}}(t_M + 1)$ to get $(t_M + 1)'$ and verifies whether $(t_M + 1)' \overset{?}{=} t_M + 1$ holds. If it does, the medical staff updates SID_M.

c: EMERGENCY PHASE

In this phase, the server responds to an accident by sending distress calls to medical staff members in order of closest proximity to the accident site. These messages are sent until one staff member confirms the assignment. The server provides continuously updated location information for the user to ensure the staff member can easily locate the user. The process is described in detail as follows (Fig. 10).

(1) The *User* extracts the time t_U, gets location loc, uses the shared key K_{SU} to encrypt them, and sends t_U, $E_{K_{SU}}(loc||t_U)$ and SID_U to the *Server*.

(2) After the *Server* receives the message, it extracts time t_S and verifies whether $t_S - t_U$ is within the expected time interval. If it is, the *Server* uses SID_U to extract ID_U and K_{SU} from *SID* table (or from *BSID* table if SID_U cannot be found from *SID* table), then uses K_{SU} to decrypt $E_{K_{SU}}(loc||t_U)$ to get loc' and t'_U, and verifies whether $t'_U \overset{?}{=} t_U$. If it does, the *Server* updates *SID* table and *BSID* table, computes $E_{K_{SU}}(m_{finding}||t_U + 1)$ before transmitting it to the *User*.

(3) The *User* uses K_{SU} to decrypt $E_{K_{SU}}(m_{finding}||t_U + 1)$ to obtain $m'_{finding}$ and $(t_U + 1)'$, and verifies whether $(t_U + 1)' \overset{?}{=} t_U + 1$ and $m'_{finding} \overset{?}{=} m_{finding}$. If it does, which means the *Server* is currently matching a medical staff for the *User*, then the *User* updates SID_U.

(4) (The *Server* finds the nearest medical staff.) The *Server* finds the nearest medical staff M_j, extracts time t_S, calculates $E_{K_{SM_j}}(m_{ask}||t_S)$ before transmitting t_S and $E_{K_{SM_j}}(m_{ask}||t_S)$ to M_j.

(5) (**Case 1 (*MS*):** The medical staff refuses to offer assistance.) Medical staff M_j obtains the message, extracts time t_{M_j}, verifies whether $t_{M_j} - t_S$ is within the regular time interval. If it is, M_j uses K_{SM_j} to decrypt $E_{K_{SM_j}}(m_{ask}||t_S)$ to obtain m_{ask} and t'_S, and verifies whether $t'_S \overset{?}{=} t_S$. If it does, M_j considers whether to offer assistance. If M_j decides to reject, it computes $E_{K_{SM_j}}(m_{reject}||t_S + 1)$ and transmits it to the *Server*.

(6) (**Case 1 (*Server*):** The *Server* receives the refuse message and finds the next nearest medical staff.) After the *Server* receives the message, it uses K_{SM_j} to decrypt $E_{K_{SM_j}}(m_{reject}||t_S + 1)$ and obtains m'_{reject} and

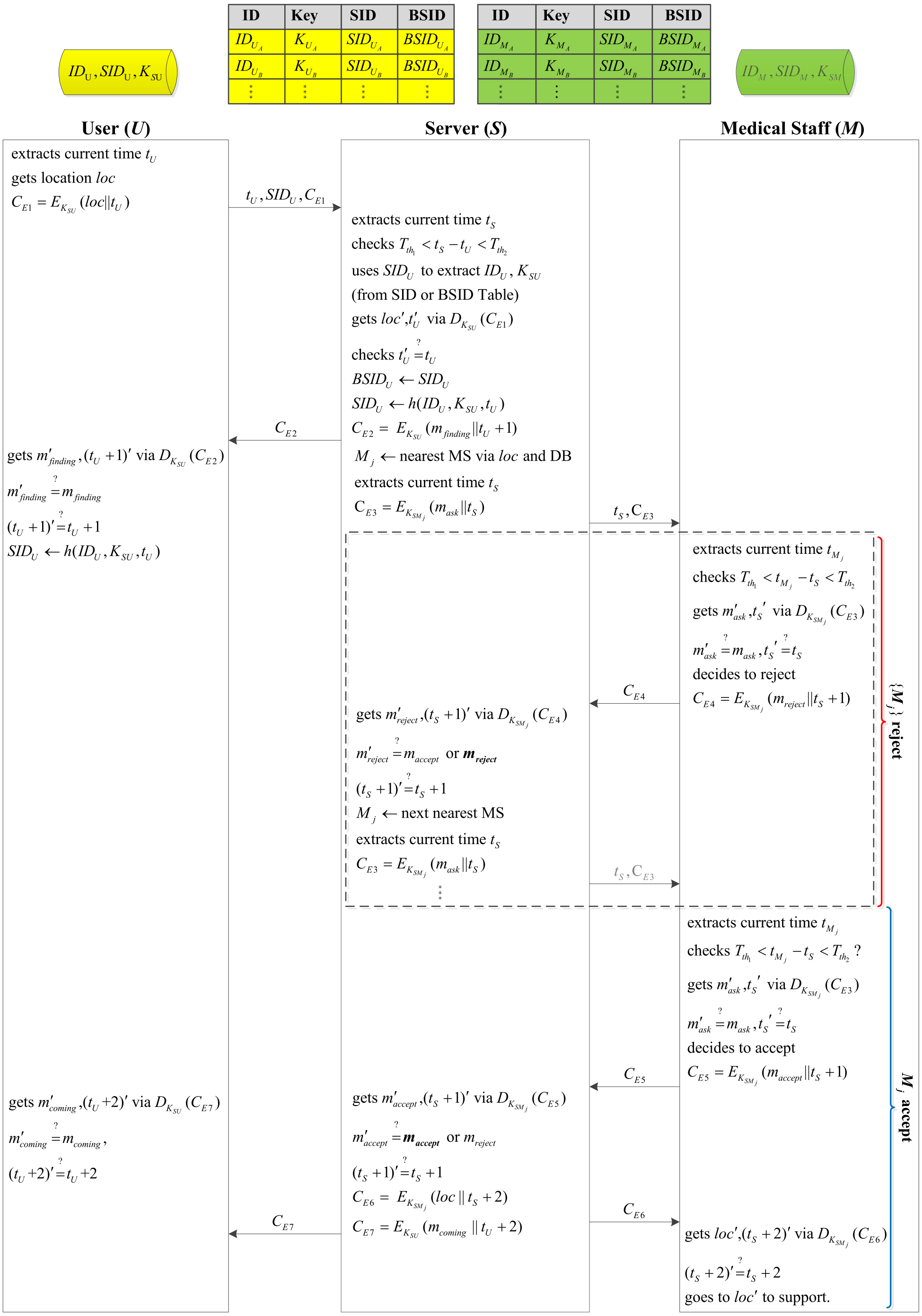

ID_U, SID_U, K_{SU}
ID | Key | SID | BSID
ID_{U_A} | K_{U_A} | SID_{U_A} | $BSID_{U_A}$
ID_{U_B} | K_{U_B} | SID_{U_B} | $BSID_{U_B}$
ID | Key | SID | BSID
ID_{M_A} | K_{M_A} | SID_{M_A} | $BSID_{M_A}$
ID_{M_B} | K_{M_B} | SID_{M_B} | $BSID_{M_B}$
ID_M, SID_M, K_{SM}
User (U)
Server (S)
Medical Staff (M)
extracts current time t_U
gets location loc
$C_{E1} = E_{K_{SU}}(loc||t_U)$
t_U, SID_U, C_{E1}
extracts current time t_S
checks $T_{th_1} < t_S - t_U < T_{th_2}$
uses SID_U to extract ID_U, K_{SU} (from SID or BSID Table)
gets loc', t'_U via $D_{K_{SU}}(C_{E1})$
checks $t'_U \overset{?}{=} t_U$
$BSID_U \leftarrow SID_U$
$SID_U \leftarrow h(ID_U, K_{SU}, t_U)$
$C_{E2} = E_{K_{SU}}(m_{finding}||t_U+1)$
C_{E2}
gets $m'_{finding}, (t_U+1)'$ via $D_{K_{SU}}(C_{E2})$
$m'_{finding} \overset{?}{=} m_{finding}$
$(t_U+1)' \overset{?}{=} t_U+1$
$SID_U \leftarrow h(ID_U, K_{SU}, t_U)$
$M_j \leftarrow$ nearest MS via loc and DB
extracts current time t_S
$C_{E3} = E_{K_{SM_j}}(m_{ask}||t_S)$
t_S, C_{E3}
extracts current time t_{M_j}
checks $T_{th_1} < t_{M_j} - t_S < T_{th_2}$
gets m'_{ask}, t_S' via $D_{K_{SM_j}}(C_{E3})$
$m'_{ask} \overset{?}{=} m_{ask}, t_S' \overset{?}{=} t_S$
decides to reject
$C_{E4} = E_{K_{SM_j}}(m_{reject}||t_S+1)$
C_{E4}
gets $m'_{reject}, (t_S+1)'$ via $D_{K_{SM_j}}(C_{E4})$
$m'_{reject} \overset{?}{=} m_{accept}$ or $\boldsymbol{m_{reject}}$
$(t_S+1)' \overset{?}{=} t_S+1$
$M_j \leftarrow$ next nearest MS
extracts current time t_S
$C_{E3} = E_{K_{SM_j}}(m_{ask}||t_S)$
t_S, C_{E3}
$\{M_j\}$ reject
extracts current time t_{M_j}
checks $T_{th_1} < t_{M_j} - t_S < T_{th_2}$?
gets m'_{ask}, t_S' via $D_{K_{SM_j}}(C_{E3})$
$m'_{ask} \overset{?}{=} m_{ask}, t_S' \overset{?}{=} t_S$
decides to accept
$C_{E5} = E_{K_{SM_j}}(m_{accept}||t_S+1)$
C_{E5}
gets $m'_{accept}, (t_S+1)'$ via $D_{K_{SM_j}}(C_{E5})$
$m'_{accept} \overset{?}{=} \boldsymbol{m_{accept}}$ or m_{reject}
$(t_S+1)' \overset{?}{=} t_S+1$
$C_{E6} = E_{K_{SM_j}}(loc || t_S+2)$
$C_{E7} = E_{K_{SU}}(m_{coming} || t_U+2)$
C_{E6}
C_{E7}
gets $m'_{coming}, (t_U+2)'$ via $D_{K_{SU}}(C_{E7})$
$m'_{coming} \overset{?}{=} m_{coming}$,
$(t_U+2)' \overset{?}{=} t_U+2$
gets $loc', (t_S+2)'$ via $D_{K_{SM_j}}(C_{E6})$
$(t_S+2)' \overset{?}{=} t_S+2$
goes to loc' to support.
M_j accept

FIGURE 10. Emergency phase.

$(t_S + 1)'$, and verifies $m'_{reject} \overset{?}{=} m_{accept}$ or m_{reject} and $(t_S + 1)' \overset{?}{=} t_S + 1$. If the verified result is m_{reject}, which denotes M_j refuse to offer assistance, the *Server* finds the next nearest medical staff M_j, extracts time t_S, and computes $E_{KSM_j}(m_{ask}||t_S)$ before transmitting t_S and $E_{KSM_j}(m_{ask}||t_S)$ to M_j.

(7) (If the medical staff refuses to offer assistance (i.e. Case 1), repeat steps (5-6).)

(8) *(Case 2 (MS):* The medical staff accepts to offer assistance.) If the medical staff M_j decides to offer assistance, it computes $E_{KSM_j}(m_{accept}||t_S + 1)$ and transmits it to the *Server*.

(9) *(Case 2 (Server):* The *Server* receives the acceptance message.) After the *Server* receives the message, it uses K_{SM_j} to decrypt $E_{KSM_j}(m_{accept}||t_S + 1)$ to obtain m'_{accept} and $(t_S + 1)'$, and verifies whether

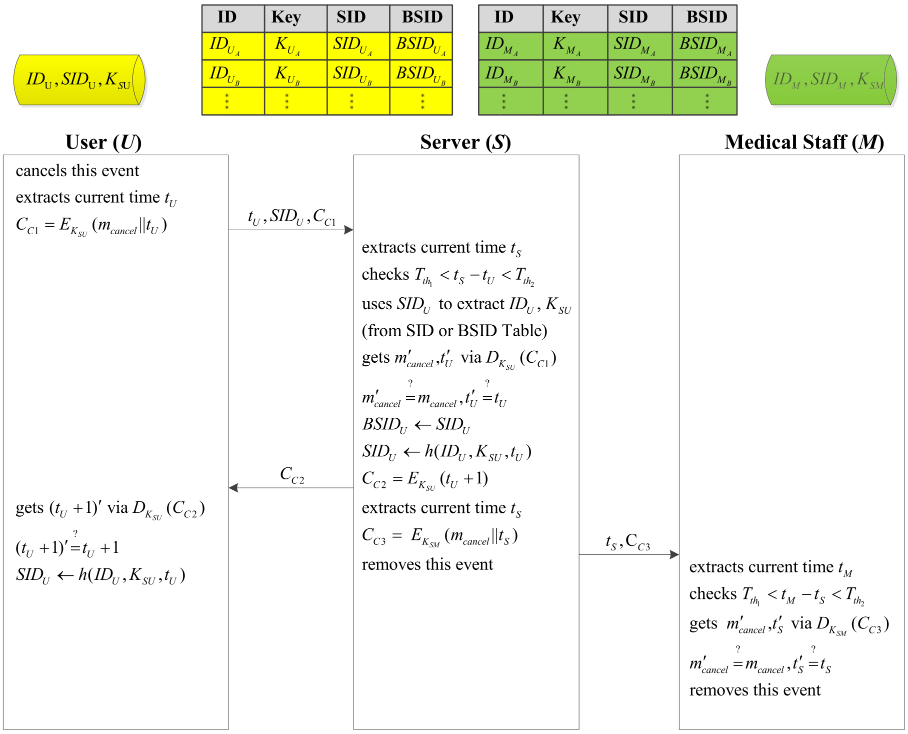

ID | Key | SID | BSID
ID_{U_A} | K_{U_A} | SID_{U_A} | $BSID_{U_A}$
ID_{U_B} | K_{U_B} | SID_{U_B} | $BSID_{U_B}$
ID | Key | SID | BSID
ID_{M_A} | K_{M_A} | SID_{M_A} | $BSID_{M_A}$
ID_{M_B} | K_{M_B} | SID_{M_B} | $BSID_{M_B}$
ID_U, SID_U, K_{SU}
ID_M, SID_M, K_{SM}
User (U)
Server (S)
Medical Staff (M)
cancels this event
extracts current time t_U
$C_{C1} = E_{K_{SU}}(m_{cancel}||t_U)$
t_U, SID_U, C_{C1}
extracts current time t_S
checks $T_{th_1} < t_S - t_U < T_{th_2}$
uses SID_U to extract ID_U, K_{SU}
(from SID or BSID Table)
gets m'_{cancel}, t'_U via $D_{K_{SU}}(C_{C1})$
$m'_{cancel} \overset{?}{=} m_{cancel}, t'_U \overset{?}{=} t_U$
$BSID_U \leftarrow SID_U$
$SID_U \leftarrow h(ID_U, K_{SU}, t_U)$
$C_{C2} = E_{K_{SU}}(t_U+1)$
C_{C2}
extracts current time t_S
$C_{C3} = E_{K_{SM}}(m_{cancel}||t_S)$
removes this event
gets $(t_U+1)'$ via $D_{K_{SU}}(C_{C2})$
$(t_U+1)' \overset{?}{=} t_U+1$
$SID_U \leftarrow h(ID_U, K_{SU}, t_U)$
t_S, C_{C3}
extracts current time t_M
checks $T_{th_1} < t_M - t_S < T_{th_2}$
gets m'_{cancel}, t'_S via $D_{K_{SM}}(C_{C3})$
$m'_{cancel} \overset{?}{=} m_{cancel}, t'_S \overset{?}{=} t_S$
removes this event

FIGURE 11. Cancel phase.

$m'_{accept} = m_{accept}$ or m_{reject} and $(t_S+1)' \overset{?}{=} t_S+1$. If the verified result is m_{accept}, which denotes M_j accept to offer assistance, the *Server* computes $E_{K_{SM_j}}(loc||t_S+2)$ and transmits it to M_j. In addition, the *Server* computes $E_{K_{SU}}(m_{co\min g}||t_U+2)$ and transmits it to the *User*.

(10) The medical staff M_j uses K_{SM_j} to decrypt $E_{K_{SM_j}}(loc||t_S+2)$ to obtain loc' and $(t_S+2)'$, and verifies whether $(t_S+2)' \overset{?}{=} t_S+2$. If it does, M_j goes to loc' and offers assistance.

(11) The *User* uses K_{SU} to decrypt $E_{K_{SU}}(m_{coming}||t_U+2)$ to obatinm'_{coming} and $(t_U+2)'$, verifies whether $m'_{coming} \overset{?}{=} m_{coming}$ and $(t_U+2)' \overset{?}{=} t_U+2$. If the verified result is correct, it denotes there is a medical staff that is going to help the *User*.

d: CANCEL PHASE

In this phase, if the user recovers on his/her own before the medical staff worker arrives, and no longer requires assistance, the user can cancel the alert, which the server will then forward to the medical staff member. This process is described in detail as follows (Fig. 11):

(1) If the *User* cancels this emergency event voluntarily, he/she extracts time t_U, computes $E_{K_{SU}}(m_{cancel}||t_U)$, and transmits t_U, $E_{K_{SU}}(m_{cancel}||t_U)$ and SID_U to the *Server*.

(2) After the *Server* receives the message, it extracts time t_S and verifies whether $t_S - t_U$ is within the regular time interval. If it is, the *Server* uses SID_U to find ID_U and K_{SU} from *SID* table (or from *BSID* table if SID_U cannot be found from *SID* table), then uses K_{SU} to decrypt $E_{K_{SU}}(m_{cancel}||t_U)$ to get m'_{cancel} and t'_U, and verifies whether $t'_U \overset{?}{=} t_U$ and $m'_{cancel} \overset{?}{=} m_{cancel}$. If it does, the *Server* updates *SID* table and *BSID* table, computes $E_{K_{SU}}(t_U+1)$ before transmitting it to the *User*. In the meanwhile, the *Server* extracts time t_S, computes $E_{K_{SM}}(m_{cancel}||t_S)$ before transmitting t_S and $E_{K_{SM}}(m_{cancel}||t_S)$ to the medical staff.

(3) The *User* uses K_{SU} to decrypt $E_{K_{SU}}(t_U+1)$ to obtain $(t_U+1)'$, and verifies whether $(t_U+1)' \overset{?}{=} t_U+1$. If it does, the *User* updates SID_U.

(4) The medical staff extracts time t_M and verify whether $t_M - t_S$ is within the regular time interval. If it is, the medical staff uses K_{SM} to decrypt $E_{K_{SM}}(m_{cancel}||t_S)$ to obtain m'_{cancel} and t'_S, and verifies whether $m'_{cancel} \overset{?}{=} m_{cancel}$ and $t'_S \overset{?}{=} t_S$. If it does, the medical staff removes this emergency event.

e: RESOLVED PHASE

In this phase, medical staff has arrived at the accident scene and have resolved the situation. The staff then alerts the server and the user that the situation is resolved. This process is described in detail as follows (Fig. 12).

(1) After the medical staff has been resolved this emergency event, it extracts time t_M and computes $E_{K_{SM}}(m_{solved}||t_M)$ before transmitting t_M, $E_{K_{SM}}(m_{solved}||t_M)$ and SID_M to the *Server*.

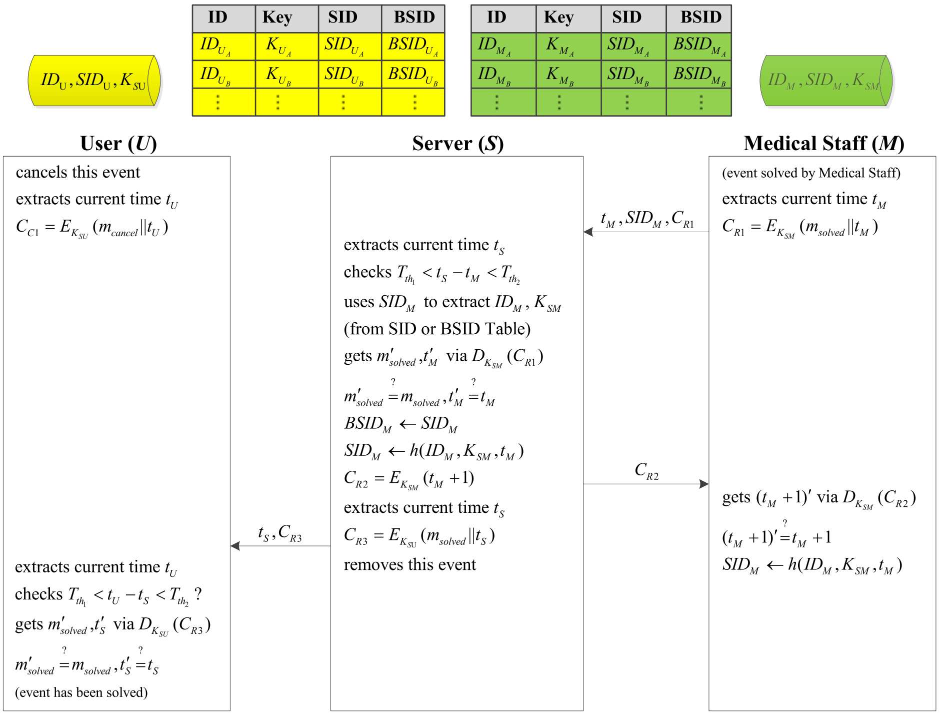

ID_U, SID_U, K_{SU}
ID | Key | SID | BSID
ID_{U_A} | K_{U_A} | SID_{U_A} | $BSID_{U_A}$
ID_{U_B} | K_{U_B} | SID_{U_B} | $BSID_{U_B}$
ID | Key | SID | BSID
ID_{M_A} | K_{M_A} | SID_{M_A} | $BSID_{M_A}$
ID_{M_B} | K_{M_B} | SID_{M_B} | $BSID_{M_B}$
ID_M, SID_M, K_{SM}
User (*U*)
Server (*S*)
Medical Staff (*M*)
cancels this event
extracts current time t_U
$C_{C1} = E_{K_{SU}}(m_{cancel} || t_U)$
(event solved by Medical Staff)
extracts current time t_M
$C_{R1} = E_{K_{SM}}(m_{solved} || t_M)$
t_M, SID_M, C_{R1}
extracts current time t_S
checks $T_{th_1} < t_S - t_M < T_{th_2}$
uses SID_M to extract ID_M, K_{SM}
(from SID or BSID Table)
gets m'_{solved}, t'_M via $D_{K_{SM}}(C_{R1})$
$m'_{solved} \overset{?}{=} m_{solved}, t'_M \overset{?}{=} t_M$
$BSID_M \leftarrow SID_M$
$SID_M \leftarrow h(ID_M, K_{SM}, t_M)$
$C_{R2} = E_{K_{SM}}(t_M + 1)$
C_{R2}
gets $(t_M + 1)'$ via $D_{K_{SM}}(C_{R2})$
$(t_M + 1)' \overset{?}{=} t_M + 1$
$SID_M \leftarrow h(ID_M, K_{SM}, t_M)$
extracts current time t_S
$C_{R3} = E_{K_{SU}}(m_{solved} || t_S)$
removes this event
t_S, C_{R3}
extracts current time t_U
checks $T_{th_1} < t_U - t_S < T_{th_2}$?
gets m'_{solved}, t'_S via $D_{K_{SU}}(C_{R3})$
$m'_{solved} \overset{?}{=} m_{solved}, t'_S \overset{?}{=} t_S$
(event has been solved)

FIGURE 12. Resolved phase.

(2) After the *Server* receives the message, it extracts time t_S and verifies whether $t_S - t_M$ is within the regular time interval. If it is, the *Server* uses SID_M to extract ID_M and K_{SM} from *SID* table (or from *BSID* table if SID_M cannot be found from *SID* table), then uses K_{SM} to decrypt $E_{K_{SM}}(m_{solved}||t_M)$ to get m'_{solved} and t'_M, and verifies whether $m'_{solved} \overset{?}{=} m_{solved}$ and $t'_M \overset{?}{=} t_M$. If it does, the *Server* updates *SID* table and *BSID* table, calculates $E_{K_{SM}}(t_M + 1)$ before transmitting it to the medical staff. In the mean while, the *Server* extracts time t_S, calculates $E_{K_{SU}}(m_{solved}||t_S)$ before transmitting t_S and $E_{K_{SU}}(m_{solved}||t_S)$ to the *User*.

(3) The medical staff use K_{SM} to decrypt $E_{K_{SM}}(t_M + 1)$ to obtain $(t_M + 1)'$, and verifies whether $(t_M + 1)' \overset{?}{=} t_M + 1$. If it does, the medical staff updates SID_U.

(4) The *User* extracts time t_U and verifies whether $t_U - t_S$ is within the regular time interval. If it is, the *User* uses K_{SU} to decrypt $E_{K_{SU}}(m_{solved}||t_S)$ to obtain m'_{solved} and t'_S, and verifies whether $m'_{solved} \overset{?}{=} m_{solved}$ and $t'_S \overset{?}{=} t_S$. If it does, the *User* removes this emergency event.

IV. COMPARISON AND SECURITY ANALYSIS

This section analyses and compares the properties and securities including the six system requirements in definition 1 and the seven security requirements in definition 2. Table 2 summarizes the comparison of both the properties and securities for the proposed *MES* and *SMES* and those schemes proposed by Glanzer [2], Berbakov *et al.* [3], Srinivasan *et al.* [4], Nie *et al.* [7], Kau and Chen [8], Moon *et al.* [12], Moon *et al.* [13], Giuliano *et al.* [19] and Ghafghazi *et al.* [21].

TABLE 2. Comparison of features and security properties.

	[2]	[3]	[4]	[7]	[8]	[12]	[13]	[19]	[21]	*MES*	*SMES*
(1-1)		v	v	v	v	v	v	v		v	v
(1-2)										v	v
(1-3)			v	v	v				v	v	v
(1-4)	v	v				v	v	v		v	v
(1-5)			semi*1			v	v	v		v	v
(1-6)					v	v	v	v	v	v	v
(2-1)									v		v
(2-2)											v
(2-3)											v
(2-4)									v		v
(2-5)									v		v
(2-6)									v		v
(2-7)									v		v

*1：Users may choose either use or disuse mobile phone during normal-operation phase

A. COMPARISON OF PROPERTIES

Our proposed systems (*MES* and *SMES*) allow the users obtain rescue at first time, and it provides six major properties.

(1-1) Provides real-time user location information: Location sensors and continuous calculations are used to derive the user's real-time coordinates which are then provided to the server.

(1-2) Instant notification of nearest available medical staff member: The server determines which staff member is in closest proximity to the accident site, ensuring shortest response time and reducing the possibility of complications due to delayed response.

(1-3) Instant notification of rescue location: The server provides medical staff with continuous location information for the user, thus minimizing response times and allowing staff to proceed directly to the accident site.

(1-4) Continuously updated medical staff location: The server continuously tracks the locations of all medical staff members, allowing the server to quickly determine the status of all staff members are optimize resources in the event of an emergency.

(1-5) No additional power requirements (in non-emergency situations): In non-emergency situations, the system works in standby mode on the user's device, drawing no additional power and thus preserving battery life.

(1-6) Ensure user location privacy (in non-emergency situations): In non-emergency situations, the system does not track user locations. All user location is protected from unintentional disclosure.

B. ANALYSIS OF SECURITY PROPERTIES FOR PROPOSED SMES

Aside from the six requirements in definition 1, *SMES* also provides seven security properties including data integrity, anonymity. authentication, location confidentiality, location unforgeability, resistance to asynchronous attacks, and resistance to tracking attacks.

1) DATA INTEGRITY

Because $E_K(loc||t_M)$ and $t'_M \overset{?}{=} t_M$ require verification, therefore if loc is changed, then $E_K(loc||t_M)$ will also change, thus the verification $t'_M \overset{?}{=} t_M$ will not succeed, and the proposed method achieves data integrity. Theorem 1 proves the property of data integrity from definition 3.

Definition 3 (Partial Message Forged Problem for Symmetric Cryptosystem): Let $X, X', Y, \in Z$, $C = E_k(X||Y)$ and $C' = E_k(X'||Y)$, where k is a symmetric encryption/decryption key, and $X' \neq X$. If C' can be evaluated from given Y and C, then we say the **partial message forged problem for symmetric cryptosystem** is solved. (The probability of solving this problem is denoted as $\Pr(C'|Y, C) = \varepsilon_1$).

Theorem 1 (Data Integrity): In our scheme, if C'_1can be evaluated and verified successfully from eavesdropped t_1 and C_1, then the **partial message forged problem for symmetric cryptosystem** can be solved, where $C_1 = E_{k_1}(m||t_1)$, $C'_1 = E_{k_1}\left(m'||t_1\right)$ and $m' \neq m$. (Note: (k_1, m, t_1) can be (K_{SU}, loc, t_U), (K_{SM}, loc, t_M), $(K_{SU}, m_{solved}, t_S)$, etc.)

Proof. In our scheme, assume an adversary tries to evaluate $C'_1 = E_{k_1}\left(m'||t_1\right)$ from eavesdropped t_1 and $C_1 = E_{k_1}(m||t_1)$, where C'_1 can be verified successfully. Let RO_1 be a random oracle: input t_1 and C_1 to output C'_1 (i.e. $RO_1(t_1, C_1) \rightarrow C'_1$.) In **definition 3**, let $t_1 \leftarrow Y$ and $C_1 \leftarrow C$ be input parameters of RO_1 and we obtain output C'_1. Let $C' \leftarrow C'_1$, then C' is evaluated. Therefore, $\Pr(C'_1|t_1, C_1) \leq \Pr(C'|Y, C) = \varepsilon_1$, which means the **partial message forged problem for symmetric cryptosystem** can be solved if RO_1 exists.

2) ANONYMITY

An attacker seeking to obtain information from both sides must use SID_A for calculations, but a one way hash function is irreversible, thus ID_A cannot be derived from $SID_A \leftarrow h(ID_A, K_{SA}, t_A)$, and the proposed method achieves anonymity. Theorem 2 proves the property of anonymity from definition 4.

Definition 4 (Partial Hash Problem): Let $a, b, c \in Z$ and $h_1 = h(a, b, c)$. If a can be evaluated from given c and h_1, then we say the **partial hash problem** is solved. (The probability of solving this problem is denoted as $\Pr(a|h_1, c) = \varepsilon_2$)

Theorem 2 (Anonymity): In our scheme, if attacker can evaluate ID_U from SID_U, then the **partial hash problem** can be solved.

Proof. In our scheme, assume an adversary tries to compute ID_U from eavesdropped SID_U and t_U. Let RO_2 be a random oracle: input SID_U and t_U to output ID_U (i.e. $RO_2(t_U, SID_U) \rightarrow ID_U$.) In **definition 4**, let $t_U \leftarrow c$ and $SID_U \leftarrow h_1$ be input parameters of RO_2 and we obtain output ID_U. Let $a \leftarrow ID_U$, then a is evaluated. Therefore, $\Pr(ID_U|SID_U, t_U) \leq \Pr(a|h_1, c) = \varepsilon_2$, which means the **partial hash problem** can be solved if RO_2 exists.

3) AUTHENTICATION

Because $t'_M \overset{?}{=} t_M$ requires verification, if an attacker establishes a new t_M or uses eavesdrops t_M, he still does not possess K to encrypt $E_K(loc||t_M)$ and thus authentication fails, and the proposed method achieves authentication. Theorem 3 proves the property of authentication from definition 5.

Definition 5 (Second Partial Message Forged Problem for Symmetric Cryptosystem): Let $X, X', Y, Y' \in Z$, $C = E_k(X||Y)$ and $C' = E_k(X'||Y')$, where k is a symmetric encryption/decryption key, $Y' \neq Y$, and X' can be either the same as or different to X. If C' can be evaluated from chosen Y' and given Y and C, then we say the **second partial message forged problem for symmetric cryptosystem** is solved. (The probability of solving this problem is denoted as $\Pr(Y', C'|Y, C) = \varepsilon_3$).

Theorem 3 (Authentication): In our scheme, if an adversary can impersonate the server, a medical staff, or a user for authentication, then the **second partial message forged problem for symmetric cryptosystem** can be solved.

Proof. In our scheme, assume an adversary tries to impersonate the server, a medical staff, or a user for authentication. S/he has to evaluate $C'_1 = E_{k_1}\left(m'||t'_1\right)$ from chosen t'_1 and eavesdropped t_1 and $C_1 = E_{k_1}(m||t_1)$, where $t'_1 \neq t_1$ and (k_1, m, t_1) can be (K_{SU}, loc, t_U), (K_{SM}, loc, t_M), $(K_{SU}, m_{solved}, t_S)$, etc. Let RO_3 be a random oracle such that

$RO_3(t_1, C_1) \rightarrow t_1', C_1'$. In **definition 5**, let $t_1 \leftarrow Y$ and $C_1 \leftarrow C$ be input parameters of RO_3 and we obtain output t_1' and C_1'. Let $Y' \leftarrow t_1'$ and $C' \leftarrow C_1'$, then Y' and C' are evaluated. Therefore, $\Pr(t_1', C_1'|t_1, C_1) \leq \Pr(Y', C'|Y, C) = \varepsilon_3$, which means the **second partial message forged problem for symmetric cryptosystem** can be solved if RO_3 exists.

4) LOCATION CONFIDENTIALITY

Because $E_K(loc||t_M)$ is encrypted with the key K which an attacker would need to obtain loc, thus the proposed method achieves location information privacy. Theorem 4 proves the property of location confidentiality from definition 6.

Definition 6 (Partial Decryption Problem for Symmetric Cryptosystem): Let $X, Y \in Z$ and $C = E_k\ (X||Y)$, where k is a symmetric encryption/decryption key. If X can be evaluated from given Y and C, then we say the **partial decryption problem for symmetric cryptosystem** is solved. (The probability of solving this problem is denoted as $\Pr(X|Y, C) = \varepsilon_4$)

Theorem 4 (Location Confidentiality): In our scheme, if attacker can evaluate loc from eavesdropped t_1 and $C_1 = E_{k_{SM}}(loc||t_1)$, then the **partial decryption problem for symmetric cryptosystem** can be solved. (Note: t_1 can stand for t_U, t_M or t_S.)

Proof. In our scheme, assume an adversary tries to evaluate loc from eavesdropped t_1 and $C_1 = E_{k_{SM}}(loc||t_1)$. Let RO_4 be a random oracle such that $RO_4(t_1, C_1) \rightarrow loc$. In **definition 6**, Let $t_1 \leftarrow Y$ and $C_1 \leftarrow C$ be input parameters of RO_4 and we obtain output loc. Let $X \leftarrow loc$, then X can be evaluated. Therefore, $\Pr(loc|t_1, C_1) \leq \Pr(X|Y, C) = \varepsilon_4$, which means the **partial decryption problem for symmetric cryptosystem** can be solved if RO_4 exists.

5) LOCATION UNFORGEABILITY

An attacker seeking to forge location information must first obtain the key K to obtain $E_K(loc||t_M)$, and thus receive server authentication through $t_M' \overset{?}{=} t_M$. However, the attacker cannot calculate K, thus the proposed method achieves location unforgeability. Theorem 5 proves the property of location unforgeability from definition 7.

Definition 7 (Forged Problem for Symmetric Cryptosystem): Let $X, Y, X', Y' \in Z$, $C = E_k\ (X||Y)$ and $C' = E_k\left(X'||Y'\right)$, where k is a symmetric encryption/decryption key, $(X', Y') \neq (X, Y)$, and $Y' \geq Y$. If C' can be evaluated from chosen X' and Y' and given Y and C, then we say the **forged problem for symmetric cryptosystem** is solved. (The probability of solving this problem is denoted as $\Pr(C', X', Y'|C, Y) = \varepsilon_5$.)

Theorem 5 (Location Unforgeability): In our scheme, if C_1'can be evaluated and verified successfully from chosen forged loc' and t_1' and eavesdropped t_1 and C_1, then the **forged problem for symmetric cryptosystem** can be solved, where $C_1 = E_{k_1}\ (loc||t_1)$, $C_1' = E_{k_1}\left(loc'||t_1'\right)$, $t_1' \geq t_1$ and $(loc', t_1') \neq (loc, t_1)$. (Note: t_1 can stand for t_U, t_M or t_S.)

Proof: In our scheme, assume an adversary tries to evaluate C_1' from chosen forged loc' and t_1' and eavesdropped t_1 and C_1. Let RO_5 be a random oracle: input t_1 and C_1 to output loc', t_1' and C_1' (i.e. $RO_5(t_1, C_1) \rightarrow loc', t_1', C_1'$.) In **definition 7**, let $t_1 \leftarrow Y$ and $C_1 \leftarrow C$ be input parameters of RO_5 and we can obtain output loc', t_1' and C_1'. Let $X' \leftarrow loc'$, $Y' \leftarrow t_1'$ and $C' \leftarrow C_1'$, then C', X' and Y' are evaluated. Therefore, $\Pr(loc', t_1', C_1'|t_1, C_1) \leq \Pr(C', X', Y'|C, Y) = \varepsilon_5$, which means the **forged problem for symmetric cryptosystem** can be solved if RO_5 exists.

6) RESISTANCE TO ASYNCHRONOUS ATTACKS

The server includes an *SID* table and a *BSID* table such that, if an attacker disrupts communications, the bilateral SID_A cannot be updated, thus SID_A is asynchronous. However, the *Server's BSID* Table stores the most recent SID_A, thus the *BSID* Table can identify the key K and identifier ID, and the proposed method is resistant to asynchronous attacks.

7) RESISTANCE TO TRACKING ATTACKS

Because $SID_A \leftarrow h(ID_A, K_{SA}, t_A)$, each communication instance will change with t_A, and the previous SID_A will have no clear relationship to the current SID_A (due to the one-way hash function), thus the proposed method is resistant to tracking attacks. Theorem 6 proves the property of resistance to tracking attacks from definition 8.

Definition 8 (Partial Pre-Hashed-Message Tracking Problem): Let $a_1, a_2, b_1, b_2, c_1, c_2 \in Z$, $h_1 = h(a_1, b_1, c_1)$ and $h_2 = h(a_2, b_2, c_2)$. If $isEqual(a_1, a_2)$ can be evaluated from given h_1, h_2, c_1 and c_2, then we say the **partial pre-hashed-message tracking problem** is solved, where $c_1 \neq c_2$ and $isEqual(a_1, a_2)$ is 0 (if $a_1 \neq a_2$) or 1 (if $a_1 = a_2$). (The probability of solving this problem is denoted as $|2\Pr(isEqual(a_1, a_2)|h_1, h_2, c_1, c_2) - 1| = \varepsilon_6$)

Theorem 6 (Resistance to Tracking Attacks): In our scheme, if an attacker can evaluate the value of $isEqual(ID_i^{(n)}, ID_j^{(m)})$ from eavesdropped $SID_i^{(n)}$, $SID_j^{(m)}$, t_1 and t_2, then the **partial pre-hashed-message tracking problem** can be solved, where $SID_i^{(n)} = h(ID_i^{(n)}, k_1, t_1)$, $SID_j^{(m)} = h(ID_j^{(m)}, k_2, t_2)$, $isEqual(x, y)$ is 0 (if $x \neq y$) or 1 (if $x = y$), and $t_1 \neq t_2$. (Note: t_1 and t_2 can stand for t_U, t_M or t_S.)

Proof: In our scheme, assume An adversary tries to track a user A from eavesdropped $SID_i^{(n)}$, $SID_j^{(m)}$, t_1 and t_2. Let RO_6 be a random oracle: $RO_6(SID_i^{(n)}, SID_j^{(m)}, t_1, t_2) \rightarrow isEqual(ID_i^{(n)}, ID_j^{(m)})$. In **definition 8**, let $SID_i^{(n)} \leftarrow h_1$, $SID_j^{(m)} \leftarrow h_2$, $t_1 \leftarrow c_1$ and $t_2 \leftarrow c_2$ be input parameters of RO_6 and we obtain output $isEqual(ID_i^{(n)}, ID_j^{(m)})$. Let $isEqual(x, y) \leftarrow isEqual(ID_i^{(n)}, ID_j^{(m)})$, then $isEqual(x, y)$ is evaluated. Therefore, $\Pr(isEqual(ID_i^{(n)}, ID_j^{(m)})|SID_i^{(n)}, SID_j^{(m)}, t_1, t_2) \leq \Pr(isEqual(a_1, a_2)|h_1, h_2, c_1, c_2)$, which means the partial pre- hashed-message tracking problem can be solved if RO_6 exists.

C. COMPARISON OF TRANSMISSION TECHNOLOGIES

In Table 3, we compare transmission technologies including Internet, WiFi, UWB, RFID, IMU, Bluetooth, Zigbee,

TABLE 3. Comparison of transmission technologies.

	[2]	[3]	[4]	[7]	[8]	[12]	[13]	[19]	[21]	*MES*	*SMES*
Entities	2^{*2}	4	4^{*5}	3	3	3	3	4	6	3	3
Internet			v		v			v	v	v	v
WiFi			v								
UWB			v^{*5}			v^{*7}	v^{*7}				
RFID			v					v			
IMU	v^{*3}	v^{*4}	v^{*5}		v^{*6}						
Bluetooth			v					v		v^{*10}	v^{*10}
Zigbee				v							
GPS	v				v	v^{*8}	v^{*8}	v^{*9}	v		
Security			v					v			v

GPS along with entities and user information security, where internet refers to WiFi or 3G/4G network. The entities in each system are first responders and person [2]; first responder, portable communication unit, track server, and authorized personnel [3]; smart building (equipped with a hybrid indoor positioning and tracking, motion detection and sensing system), community cloud, emergency service provider, and emergency responder [4]; ZigBee, underground personnel, and physiological indicators [7]; the smart phone-based pocket fall accident detector, the coordination center, and the rescue center [8]; portable access points (consisted of two ranging devices: anchor and tag), monitor station, and firemen [12]; portable access points (consisted of two ranging devices: anchor and tag), monitor station, and first responders [13]; RFID Tag, RFID Reader, User device, and Remote command and control center [19]; key generation authority, public safety answering point, cloud server, data owners, first responders, and tamper proof GPS [21]; and user, medical staff, and server [MES/SMES].

The indications of asterisks are shown as follows. *2: This paper suggests two integrated positioning system architectures for first responders and person. *3: IMU-based systems are suggested for indoor first-responder positioning, while pedometer and compass are suggested for indoor personal positioning. *4: A step detection algorithm is used and current heading of a person is found by using the magnetometer and the gyroscope. *5: A smart building is equipped with a hybrid system. *6: Fall accident detector uses IMU-based sensors. *7: The two ranging devices (anchor and tag) in each AP follow the IEEE 802.15.4a standard, which specifies four different PHYs (three of which utilized direct-sequence spread spectrum (DSSS), and one which used parallel-sequence spread spectrum (PSSS)) and two additional PHYs (using ultra-wideband (UWB) and chirp spread spectrum (CSS)). *8: It is assumed that the monitoring station is the origin of the whole positioning system and given by the conventional GPS. *9: User Device can exploit the available embedded chipset to calculate its outdoor position (through A-GPS or GPS) as well as to integrate the indoor localization procedure. *10: It depends on the positioning method, such as Bluetooth-based beacon positioning method.

V. IMPLEMENTATION

This section presents the implementation of the proposed *MES* and *SMES*. We use one personal computer and two android phones to implement a server, a user and a medical staff respectively. In addition, we use Estimote's beacons to offer the locational information. The personal computer implementation used Windows 8.1 with an Intel (R) core (TM) i5-2400CPU @ 3.10GHz and 4G RAM. Android phone implementation used HTC Desire 816 based on Android 5.0 and Qualcomm S400 1.6GHz. Moreover, the hash function used is SHA-256 [24], the symmetric encryption algorithm is AES [25]. Table 4 compares the performance (including computation and communication cost) between each phases of our *SMES* to show their efficiency, Table 5 shows the average implementation time in each phase.

TABLE 4. Computation and communication costs.

	Normal-operation phase			Emergency phase			Cancel phase			Resolved phase		
	U	*M*	*S*	*U*	*M*	*S*	*U*	*M*	*S*	*U*	*M*	*S*
Encryption / Decryption	0	2	2	3	5	8	2	1	3	2	2	3
Hash	0	1	1	1	0	1	1	0	1	0	1	1
Transmission messages	0	3	1	3	2	7	3	0	3	0	3	3
Transmission rounds	0	1	1	1	2	5	1	0	2	0	1	2

TABLE 5. Implementation time.

Phases	Time
Register phase	25ms
Normal-operation phase	95ms
Emergency phase (medical staff has been assign)	104ms
Cancel phase	110ms
Resolve phase	90ms

In our implementation, we assume that the system time of the server and two Android phones are synchronized. However, the system times on the server and the Android phones are difficult to be synchronized. Fortunately, the experience in implementation shows that the system time difference between the server and the phones is within mini seconds. By assuming the maximum system time difference between the server and phones is 1000 mini seconds, and the value $t_S - t_M$ is between 10 ms and 30 ms, we suggest to set T_{th_1} and T_{th_2} to −990 ms and 1030 ms, respectively. (In real situation, the value $t_S - t_M$ is suggested to be measured again for much accuracy.)

VI. CONCLUSION

Aging societies are increasing demands on understaffed nursing homes and care facilities, creating a critical need for optimal efficiency. This paper proposes a mobile emergency call and the nearest rescuer information system with privacy and authentication, which provides six system requirements and seven security requirements (including data integrity, anonymity. authentication, location confidentiality, location unforgeability, resistance to asynchronous attacks, and resistance to tracking attacks). Compared with other schemes, only our schemes provide the system property: instant notification of nearest available medical staff member. Moreover, most scheme do not supply any security characteristics while our SMES scheme provide six security properties (along with security proves via a formal security proving model), including two special security properties: anonymity and authentication, which are only offered by SMES scheme. The proposed system was implemented in Android and Windows, can complete the emergency phase and the resolve phase in only 104ms and 90ms in average, and can significantly improve patient safety in homes, hospitals and other care facilities. Future work will focus on further developing related applications to enhance hospital care environments and improve long-term care conditions.

REFERENCES

[1] A. S. Bastos, V. Vieira, and A. L. Apolinario, Jr., "Indoor location systems in emergency scenarios: A Survey," in *Proc. Annu. Conf. Brazilian Symp. Inf. Syst., Inf. Syst., Comput. Socio-Tech. Perspective, Brazilian Comput. Soc.*, vol. 1, 2015, p. 34.

[2] G. Glanzer, "Personal and first-responder positioning: State of the art and future trends," in *Proc. Ubiquitous Positioning, Indoor Navigat., Location Based Service (UPINLBS)*, Oct. 2012, pp. 1–7.

[3] L. Berbakov, B. Pavkovic, and S. Vrane, "Smart indoor positioning system for situation awareness in emergency situations," in *Proc. 26th Int. Workshop Database Expert Syst. Appl. (DEXA)*, Sep. 2015, pp. 139–143.

[4] R. Srinivasan, A. Mohan, and P. Srinivasan, "Privacy conscious architecture for improving emergency response in smart cities," in *Proc. Smart City Security Privacy Workshop (SCSP-W)*, vol. 2016, pp. 1–5.

[5] D.-M. Do, M.-H. Hyun, and Y.-B. Choi, "RFID-based indoor location recognition system for emergency rescue evacuation support," in *Proc. Int. Conf. Grid Pervas. Comput.*, 2013, pp. 899–906.

[6] N. Li, B. Becerik-Gerber, B. Krishnamachari, and L. Soibelman, "A BIM centered indoor localization algorithm to support building fire emergency response operations," *Automat. Construction*, vol. 42, pp. 78–89, Jun. 2014.

[7] B.-S. Nie, W.-X. Chen, L.-K. Wang, R.-M. Zhang, and C. Wang, "Internet of things-based positioning of coalmine personnel and monitoring of emergency state," in *Proc. 2nd Int. Conf. Digit. Manuf. Automat. (ICDMA)*, Aug. 2011, pp. 657–660.

[8] L.-J. Kau and C.-S. Chen, "A smart phone-based pocket fall accident detection, positioning, and rescue system," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 1, pp. 44–56, Jan. 2015.

[9] V. Liutkauskas, D. Matulis, and R. Pleštys, "Location Based Services," *Elektronika Elektrotechnika*, vol. 52, no. 3, pp. 35–40, 2004.

[10] A. Amanatiadis, A. Gasteratos, and D. Koulouriotis, "An intelligent multisensor system for first responder indoor navigation," *Meas. Sci. Technol.*, vol. 22, no. 11, p. 114025, Nov. 2011.

[11] K. Hari, J.-O. Nilsson, I. Skog, P. Händel, J. Rantakokko, and G. Prateek, "A prototype of a first-responder indoor localization system," *J. Indian Inst. Sci.*, vol. 93, no. 3, pp. 511–520, 2013.

[12] G. B. Moon, M. B. Hur, and G.-I. Jee, "An indoor positioning system for a first responder in an emergency environment," in *Proc. 12th Int. Conf. Control, Autom. Syst. (ICCAS)*, Oct. 2012, pp. 1368–1372.

[13] G. B. Moon, S. Chun, M.-B. Hur, and G.-I. Jee, "A robust indoor positioning system using two-stage EKF SLAM for first responders in an emergency environment," in *Proc. 13th Int. Conf. Control, Autom. Syst. (ICCAS)*, Oct. 2013, pp. 707–711.

[14] F. Pascucci *et al.*, "A REference implementation of interoperable indoor location & communication systems for First REsponders: The REFIRE project," in *Proc. IEEE Int. Symp. Safety, Secur., Rescue Robot. (SSRR)*, Nov. 2012, pp. 1–5.

[15] J. Rantakokko *et al.*, "Accurate and reliable soldier and first responder indoor positioning: Multisensor systems and cooperative localization," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 10–18, Apr. 2011.

[16] R. Zhang, F. Hoflinger, and L. Reindl, "Inertial sensor based indoor localization and monitoring system for emergency responders," *IEEE Sensors J.*, vol. 13, no. 2,, pp. 838–848, Feb. 2013.

[17] F. Pascucci and R. Setola, "An indoor localization framework for hybrid rescue teams," *IFAC Proc. Vol.*, vol. 44, no. 1, pp. 4765–4770, 2011.

[18] L. Zhang, S. Alkobaisi, W. D. Bae, and S. Narayanappa, "Ultra wideband indoor positioning system in support of emergency evacuation," in *Proc. 5th ACM SIGSPATIAL Int. Workshop Indoor Spatial Awareness*, 2013, pp. 42–49.

[19] R. Giuliano, F. Mazzenga, M. Petracca, and M. Vari, "Indoor localization system for first responders in emergency scenario," in *Proc. 9th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jul. 2013, pp. 1821–1826.

[20] X. Zhou, H. Zhang, and L. Sun, "Research on location technology in building fire rescue," *AASRI Procedia*, vol. 3, pp. 445–450, 2012.

[21] H. Ghafghazi, A. Elmougy, H. T. Mouftah, and C. Adams, "Location-aware authorization scheme for emergency response," *IEEE Access*, vol. 4, pp. 4590–4608, 2016.

[22] H. Zhu, R. Lu, C. Huang, L. Chen, and H. Li, "An efficient privacy-preserving location-based services query scheme in outsourced cloud," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7729–7739, Sep. 2016.

[23] W. Yu, Z. Liu, C. Chen, B. Yang, and X. Guan, "Privacy-preserving design for emergency response scheduling system in medical social networks," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 1, pp. 340–356, 2016.

[24] Elar. (2017). *Java JS SHA-256*. [Online]. Available: http://www.cnblogs.com/elaron/archive/2013/04/09/3010375.html

[25] hbcui1984. (2017). *The Implementation of AES Encryption in JAVA*. [Online]. Available: http://blog.csdn.net/hbcui1984/article/details/5201247

[26] ICP DAS Co. (Apr. 2017). *WLS-Analyzer Wireless Locating System Software—M2M-ICP DAS*. [Online]. Available: ftp://ftp.icpdas.com.tw/pub/cd/usbcd/napdos/wls_series/manual/wls-t02_quickstart_0100_en.pdf

[27] T. G. Zimmerman, "Personal area networks: Near-field intrabody communication," *IBM Syst. J.*, vol. 35, nos. 3–4, pp. 609–617, 1996.

[28] M. R. Yuce, "Implementation of wireless body area networks for healthcare systems," *Sens. Actuators A, Phys.*, vol. 162, no. 1, pp. 116–129, 2010.

[29] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017, doi: 10.1109/JSYST.2016.2544805.

[30] B. Kang, J. Wang, and D. Shao, "Certificateless public auditing with privacy preserving for cloud-assisted wireless body area networks," *Mobile Inf. Syst.*, vol. 2017, Jul. 2017, Art. no. 2925465.

[31] G. X. Xu, Q. Wu, M. Daneshmand, Y. Liu, and M. M. Wang, "A data privacy protective mechanism for wireless body area networks," *Wireless Commun. Mobile Comput.*, vol. 16, pp. 1746–1758, Nov. 2016.

[32] M. Toorani. (2015). "On vulnerabilities of the security association in the IEEE 802.15.6 standard." [Online]. Available: https://arxiv.org/abs/1501.02601

[33] M. Toorani, "Cryptanalysis of two PAKE protocols for body area networks and smart environments," *Int. J. Network Secur.*, vol. 17, no. 5, pp. 629–636, 2015.

SHIN-YAN CHIOU received the Ph.D. degree in electrical engineering from National Cheng Kung University, Taiwan, in 2004. From 2004 to 2009, he was a Research and Development Engineer with the Industrial Technology Research Institute. Since 2009, he has been with the Faculty of the Department of Electrical Engineering, Chang Gung University, Taoyuan, Taiwan, where he is currently an Associate Professor. His research interests include information security, cryptography, social network security, and secure applications between mobile devices.

ZHEN-YUAN LIAO received the B.S. degree from the Department of Electrical Engineering, Chang Gung University, in 2016, where he is currently pursuing the master's degree with the Graduate School of Electrical Engineering. His research interests include information security and secure applications in mobile devices.