International Research Journal of Computer Science (IRJCS)
Issue 7, Volume 2 (July 2015)
ISSN: 2393-9842
www.irjcs.com

An Enhanced Location Registration Strategy Effective for Emergency Situations

Jung Suk Joo*
Dept. of Electronics Engineering ,
Hankuk University of Foreign Studies, Korea

Abstract— In wireless mobile cellular systems, it has been popular for mobile units to support some short-range wireless communication protocols (SRWCPs)−Bluetooth, Zigbee, NFC (near field communication), etc. Thus, mobile units can easily communicate with adjacent mobile units under an SRWCP without using cellular protocols. In this paper, we introduce a simple SRWCP-aided location registration scheme in which information on adjacent mobiles is reported together with its own location to the base station: before executing a location registration process, a mobile unit tries to communicate with adjacent mobile units by using an SRWCP, and reports the information on them also. Then, in emergency cases, it is possible to get information about major figures (a suspect, witnesses, etc), since they may stay close to the user (or victim).

Keywords— ***Location Registration, Short Range Wireless Communication Protocol, Emergency Preparedness***

I. INTRODUCTION

In order to correctly deliver calls, wireless mobile cellular systems should keep track of the location of each mobile unit. For this, every mobile unit periodically registers its current location information, which is stored/updated in location databases [1]. Recently, aside from this original purpose, the location information is frequently used for the purpose of tracking down a user's (or victim's) location in case of emergency.

Unlike mobile ad hoc networks (or sensor networks) where nodes communicate with each other for neighboring sensing [2], mobiles in wireless mobile cellular systems communicate only with base stations under cellular protocols—that is, the conventional cellular systems do not have any information about adjacent mobiles of the desired user. Thus, if the user's mobile unit is forcibly switched off in an emergency situation, further tracking of its location is impossible.

How can we get information about major figures—a victim, a suspect, witnesses, etc—in case the user's mobile unit was forcibly switched off? It has been popular for mobile units to support some short-range wireless communication protocols (SRWCPs: Bluetooth, Zigbee, NFC, etc), and thus mobile units can easily communicate with adjacent mobiles under an SRWCP, without using cellular protocols [3],[4]. If mobiles periodically report information about adjacent mobiles obtained by using an SRWCP, the most recent information about adjacent mobiles can be stored/updated in the system, and in emergency cases it can give important clues on major figures since they may stay close to the user. Based on this, in this paper, we propose an SRWCP aided location registration strategy where information on adjacent mobiles is also reported: 1) before executing a location registration process, a mobile unit tries to communicate with adjacent mobile units by using an SRWCP; 2) if a connection is established, it requests and receives the identification number of the adjacent mobile (under an SRWCP); 3) it reports information on adjacent mobiles as well as its own location (under a cellular protocol).

II. PROPOSED LOCATION REGISTRATION STRATEGY

We propose a location registration scheme in which information on adjacent mobile units is gotten using an SRWCP which recent mobile units generally support and such information is registered together when registering location. The proposed location registration scheme is depicted in Fig.1, where the mobile unit, MU_1 tries to execute location registration under a cellular protocol.

A. Location Registration Procedure

The operation procedure of the proposed scheme is as below.

step1: Before registering location, attempt to communicate with adjacent mobiles using an SRWCP.

step2: If the connection is established using an SRWCP, request and receive the unique identification number of this adjacent mobile unit through an SRWCP. For protecting privacy, identification numbers should be encrypted. In Fig.1, three adjacent mobiles (MU_2, MU_3, and MU_4) are connected, and their encrypted IDs (A_2, A_3, and A_4) are sent to the MU_1 under an SRWCP.

step3: When performing location registration, report the encrypted identification numbers of adjacent mobile units together with its own location to the base station. In Fig.1, the location information of the MU_1 is reported in the form of [MU_1 *Location*, A_2, A_3, A_4], where the encrypted identification numbers are decrypted by the base station and then updated in the location databases.

Of course, in the case where there are multiple mobile units which were connected through an SRWCP, the pre-defined number of mobile units is registered in order of strong receive sensitivity—determining that the stronger receive sensitivity a mobile unit has, the closer it is located.

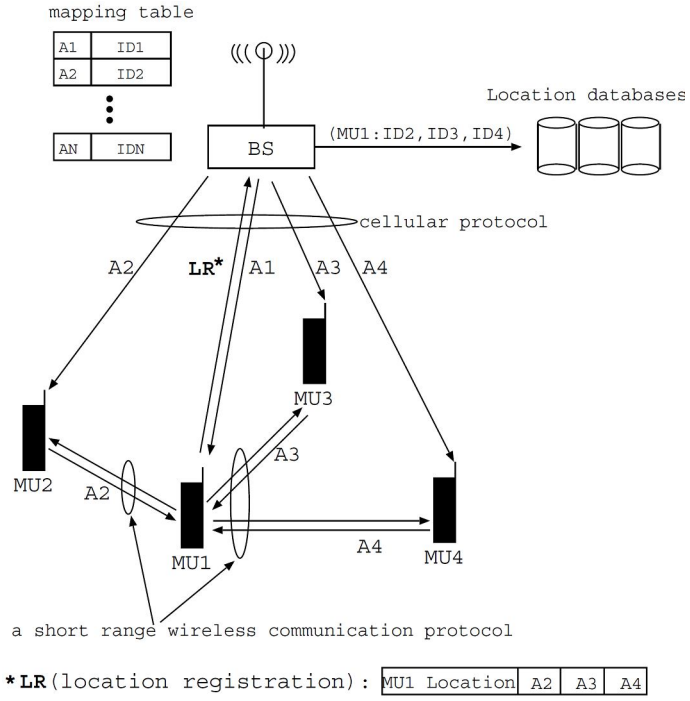

Fig. 1 Proposed location registration scheme.

B. An Example of Encryption/Decryption: Using Virtual Codes

For the proper operation of the proposed scheme, an SRWCP connection and exchange of identification numbers should be mandatory for every mobile unit through legal regulation. Thus, privacy protection is one of the most important issues.

First, location databases should be secured by having them be accessed only when the authorities allow it. Second, the mobile unit performing a location registration should not know and/or utilize identification numbers of adjacent mobile units. As a simple solution, we can consider encryption/decryption using virtual codes the concept of virtual codes has been often used in internet protocol (IP)-based networks [5],[6]. The base station prepares a mapping table in which the virtual codes and the corresponding identification numbers can be stored. Whenever a mobile unit, MU_i whose identification number is ID_i comes into a serving cell of the base station, the base station assigns a virtual code, A_i to the mobile unit and stores (A_i , ID_i) pairs in the mapping table (see Fig.1). If a mobile unit is requested to send its identification number through an SRWCP, then it sends the virtual code instead of the identification number.

Since only virtual codes are sent/received among mobile units through an SRWCP, mobile units cannot know the identification numbers of adjacent mobile units. When registering location, a mobile unit only sends its location information with adjacent mobiles' virtual codes to the base station. After finding the identification numbers corresponding to the reported virtual codes by using the mapping table, the base station updates both the mobile unit's location and the adjacent mobiles' identification numbers in location databases. Thus, it is possible to get the most recent information about adjacent mobiles—only when the authorities allow to access location databases, after carefully investigating whether a given situation is emergent or not.

III. CONCLUSION

Motivated by the fact that the recent mobile units in cellular systems generally support some SRWCPs, we proposed an SRWCP aided location registration scheme where information on adjacent mobiles obtained by using an SRWCP is reported together with location information; that is, it is based on the interoperation of a cellular protocol and an SRWCP. In addition, for the purpose of privacy protection, a simple encryption/decryption process using virtual codes was described. In emergency cases, the information on the adjacent mobiles can be used as an important clue about major figures, and it would also help to predict the location in case the user's mobile unit was forcibly switched off.

Although the proposed scheme needs some legal regulation and has some implementation issues, we expect that the proposed scheme can be considered as an attempt to solve a social problem (here, a disappearance or abduction) by using information communication technology (ICT).

ACKNOWLEDGMENT

This work was supported by Hankuk University of Foreign Studies Research Fund of 2014.

REFERENCES

[1] V. W. -S. Wong and V. C. M. Leung, "Location management for next-generation personal communications networks," *IEEE Network Magazine*, vol.82, no.9, pp.18-24, Sep./Oct. 2000.

[2] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wireless Commun.*, vol.14, pp.85-91, Oct. 2007.

[3] F. H. P. Fitzek, M. Katz, and Q. Zhang, "Cellular controlled short-range communication for cooperative P2P networking," *Wireless Personal Commun.*, vol.48, pp.141-155, Jan. 2009.

[4] C. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol.10, no.8, pp.2752-2763, Aug. 2011.

[5] C. So-In, R. Jain, S. Paul, and J. Pan, "Virtual ID: A technique for mobility, multi-homing, and location privacy in next generation wireless networks," *Proc. 7th IEEE Consumer Communications and Networking Conference (CCNC 2010)*, Las Vegas, USA, pp.1-5, Jan. 2010.

[6] S. Jain, Y. Chen, Z. Zhang, and S. Jain, "VIRO: a scalable, robust and namespace independent virtual id routing for future networks," *Proc. 30th IEEE International Conference on Computer Communications (INFOCOM 2011)*, Shanghai, China, pp.2381-2389, April 2011.