Positionally Exclusive Broadcasting

Tomáš Žižka, Athanasios Podaras
Department of Informatics
Faculty of Economics, Technical University of Liberec
Voroněžská 13, Liberec, Czech Republic
tomas.zizka@tul.cz, athanasios.podaras@tul.cz

Abstract— **Early information distribution in crisis events constitutes an important life-saving and social security characteristic. Modern information technologies can provide the possibility of developing systems which can timely send warning messages to citizens within a specific area in order to protect them from a crisis event that occurs in a close region. The current paper attempts to design a new system model aimed to be utilized for warning citizens outside a building about criminal activity in the inner part, within a target area, and prevent them from entering inside. Basic parts of the proposed early-warning system are the RADIO-HELP system enriched by an algorithmic message encryption/decryption process. Combination of these methodologies forms the proposed contribution. People inside the building shall receive by the Police Operational Center encrypted message so that no panic situation will occur and no escape effort will be made by criminals; on the other hand citizens outside the building shall receive clear decrypted message. The message type (encrypted or decrypted) is dependent on the geographic definition of the target area.**

Keywords-broadcasting; decryption; emergency; encryption; information; RADIO-HELP.

I. INTRODUCTION

The transmission of relevant information during non-standard - special and unexpected - situations to demanded places has been always considered to be an important task. However, in today's "modern world", where the development of information technology is rapid, multiple advanced technical resources that can assist in the early and timely distribution of critical and important information to desired locations exist. But, as it turned out in the recent past, the transmission of necessary and sometimes vital information in crisis situations (floods in the Czech Republic in 2013, leakage of hazardous sludge from the aluminum processing plant in western Hungary in October 2010, etc.) was not always effective or failed completely [1][2].

At first, it is necessary to define what can be considered as non-standard situation. This term can include emergencies, crises and other situations that may affect the normal status of life of a certain group of people [3].

Emergency can be defined as an event or situation that is in a certain environment caused by natural disasters, accidents, criminal activity, threats to critical infrastructure, disease, threats to internal security and economy [4]. Examples of emergencies are fires, floods, storms, traffic accidents, plane crash and threats against public safety as a result of criminal and terrorist events and so on.

As a consequence, the question is how could we effectively use available technology to ensure that in case of an emergency or crisis situation, important information will be delivered to concerned recipients on time, in an understandable form and moreover only to locations where the concrete message will be useful.

The aim of this paper is to outline possible methods of distributing information in emergency situations that, additionally, require data encryption, so that they are readable only in a certain location/position. Safety support during criminal activity or terrorist attacks is one of the areas where information coding based on the position of the receiver could be extremely useful.

The rest of the paper is structured as follows: The starting point of the proposed solution is a model situation that is described in the Section II-A. Section II-B mentions the basic system requirements. Section III-A gives information about RADIO-HELP system [5][6], which constitutes the basic building block for the design of a system for distributing positionally encrypted information. Section III-B provides basic attributes of the encrypted positional broadcasting. Details about model of the message transmitting procedure are given in Section IV. The paper closes with a summary in Section V.

II. MODEL SITUATION AND BASIC REQUIREMENTS

A. *Model Situation*

A wanted criminal is spotted at a certain shopping center. The Czech Police coordinates the measures needed to be taken in order to secure safety within the shopping center. Moreover, a critical police task is to warn the citizens, who are approaching the given shopping center and advise them to avoid the area. Therefore, it is necessary to define the message target area with regard to the shopping center, so that only people located outside the defined region will obtain the broadcasted police warning. As the flow of information within the center is coordinated by the police, the possibility of confusing the shoppers inside the center with a transmitted message aimed for another group must be eliminated, because this could cause a panic. It is also important that messages distributed through this information channel will be kept secret from criminals.

ISBN: 978-1-61208-309-4

A graphical representation of a model situation is shown in Fig. 1. The area where it should be received decrypted message (clear warning message) is marked in green. Area of shopping center and gray colored circle are areas for which the message is encrypted. The location of an armed criminal is marked in Fig. 1 with red color.

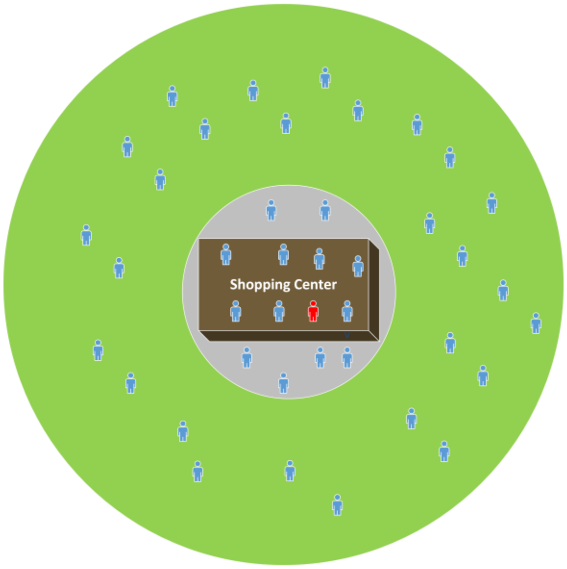

Figure 1. Graphical representation of a model situation

B. *System Requirements*

The idea of a transmitting encrypted information based on the position, does not aim to develop a completely new system, but to use existing technology components and solutions that will, however, be integrated to new functional units.

The basic requirements are the following:

- Information must be available to everyone (citizens, visitors, etc.) who is inside the target area,
- The ability to encrypt information, based on geographic definition of the target area,
- Independence of the functionality of mobile networks and the Internet,
- The information provider must be a reputable source,
- Security and robustness of the system against abuse,
- The possibility of ongoing testing and verification of functionality.

III. Technical Attributes of the Encrypted Positional Broadcasting

The basis of the proposed system for encrypted positional broadcasting is the use of system called RADIO-HELP [5][6], which is designed and developed at the Department of Informatics of the Technical University of Liberec in Czech Republic.

The aim of the present research team is to create a modern and innovative early warning system that will inform citizens that a crisis event due to criminal activity takes place within a specific area.

More precisely, the currently described methodology will be based on the combination of two tested scientific tools. The first tool is the RADIO – HELP system, an innovative message broadcasting instrument that utilizes both digital and analogue technology.

The second tool that will be utilized as an additive feature to the above mentioned technology, with the ambition to result in the formulation of a modern and innovative application, is the position based encryption/decryption algorithm. The location based encryption algorithmic procedure is also delineated and utilized by multiple researchers who have already developed and tested its functionality on mobile users.

Scott and Denning [7] proposed a data encryption suggested a data encryption algorithm by using the GPS called Geo-Encryption, the functionality of which is based on the traditional encryption system and communication protocol. For the sender the encryption was encrypted according to the PVT (Position, Velocity, Time) of the receiver.

Futhermore, Liao et al. (2008) [8] introduced and proposed the Location – Dependent Data Encryption Algorithm (LDEA). The position based encryption concept is also inspired from a similar approach called Location Based Services (LBS), the importance of which is underlined and thoroughly analyzed by Mohopatra and Suma (2005).

Location Based Services are classified in four categories [9]:

- Emergency service
- Information service
- Tracking service
- Entertainment Service

Taking into consideration the emergency and information service categories and also the target operation of the functionality defined by the present work, it can be realized that a prospective encryption algorithm dependent on the position of the mobile user will be derived from existing similar algorithmic approaches in order to extend the RADIO-HELP functionality and ameliorate the prevention of criminal actions within a target area.

A. *Description of RADIO-HELP System*

Detailed principle of RADIO-HELP system is described in [10] under the working title RADIO-H (RADIO-HELP). It is based on simultaneous application of analogue broadcasting technology with superposition of digital content (HD RADIO or DRM) or full-digital broadcasts with the possibility of defining the positional coordinates via GPS [5] [6]. HD Radio technology company iBiquity Digital Corporation was selected in 2002 in the U.S. as a key technology for the digitization of radio broadcasting. Currently, this technology carries a large percentage of U.S.

radio stations. More information about HD Radio Broadcasting is described in [11].

HD Radio technology uses the principle of superposition of the digital signal to analogue signal. The transmitted relation of Radio-Help uses positional codes for identifying areas of compulsory income, i.e., where the broadcast is directed. The receiver in the area is maintained in a standby mode and captured broadcast on fixed rate compares its position according to GPS coordinates with areas included in the broadcast. If there is compliance, it activates forced broadcast reception session. After the broadcasting code ends, the receiver goes into standby mode again. Subscribers of RADIO-HELP that are outside the defined zone will not be disturbed by warning broadcast sessions.

This principle implies that it is possible to transmit separate sessions to more areas simultaneously. Long wave radio transmitters, which with new higher quality broadcasting channels gradually lose their utility, could be used for the broadcast. In such a case, it would suffice to cover the whole Czech Republic just by one central long wave radio sender [12].

Due to the development of IT where circuits for terrestrial broadcasting and positioning GPS are now equipped with most new mobile phones, it should not be technically demanding to use it for purposes of positionally based broadcasting.

B. Basic Attributes of the Encrypted Positional Broadcasting

The concept of the proposed model relies on the early warning broadcasted messages to citizens within and outside a defined area, where criminals and suspects are spotted by the police, and police actions against the latter is about to take place. The core characteristic of the transmitted messages is that they must be based on position. As a consequence, the data sent inside the defined area where criminals are found in the certain moment, will differ from the data content which will refer to the people who are at that time outside this area. In other words, the broadcasted warning message has to be sent as encrypted (i.e., ciphertext) when it is addressed to the citizens inside the target area and as plaintext or decrypted in the case that it is addressed to the people found outside the same area.

It can be, thus, realized that the algorithmic approach which is related to the encryption/decryption procedure of the early warning messages is comprised of the following steps: a) encryption of the broadcasted message and b) decryption of the message when i.e. the mobile user is found outside the region.

Multiple message encryption/decryption algorithmic approaches exist, such as the symmetric, asymmetric, hybrid and GeoEncryption [7]. The contribution described in the present paper, should be based on GeoEncryption algorithm, since it is an approach that takes into consideration the location of receiver, which is core characteristic of the desired system. However, the final algorithmic encryption strategy, which will be added to RADIO-HELP system in order to formulate the target contribution, will be decided in future part of the research.

The aforementioned area can be a shopping center, a park, a hospital, a public organization or even a square. When police receives information about the presence of a criminal in a shopping center the immediate action that should be taken according to our proposed model, in order to protect the lives of citizens and succeed in eliminating the danger to which they could be exposed, is comprised of the below described procedure.

IV. Model of the Message Transmitting Procedure

The final critical step of the system's conceptual construction was the flow specification of the broadcasting process of the so called early warning messages. As soon as the criminal's presence (i.e., in Shopping Center) is realized by the Police, there will be an immediate broadcast of a warning message to the citizens who are at that moment inside the area (center) and at the same time for those citizens who are outside the area so that they will not attempt to visit the defined region. In the second case, the message is characterized as the early warning protection message. The model's flow with regard to the early warning message transmission is depicted in Fig. 2. The transmission procedure is initiated by Message encryption. The warning text message is formulated and then encrypted.

In the next step, it is necessary to define the target region of the warning message as well as the area for which the message is encrypted with a special algorithm based on GPS coordinates related to this area.

The third step of the process is the transition of the encrypted message from the Police Operation Center to a special transmitter. If the transmitter does not reject the incoming message due to a technical problem, the same message will be sent at once to citizens' mobiles, radios, car radios and other possible devices in a form of text. For the user group placed inside the target area the broadcasted message, due to encryption, will be displayed as advertising text so that it will not be understood by criminals as warning message from the Police. Moreover, this form of text will help the police take action without the cause of panic to citizens. Panic situation will be avoided since this group of end users will obtain the same encrypted message in the form of advertisement.

However, the message, as it was above stated, will be also addressed to a second group of people outside the defined area. In this case it will be decrypted and displayed in its original form as a clear warning text. As a result the second group will be successfully and timely informed of the forthcoming danger and will avoid the specific area.

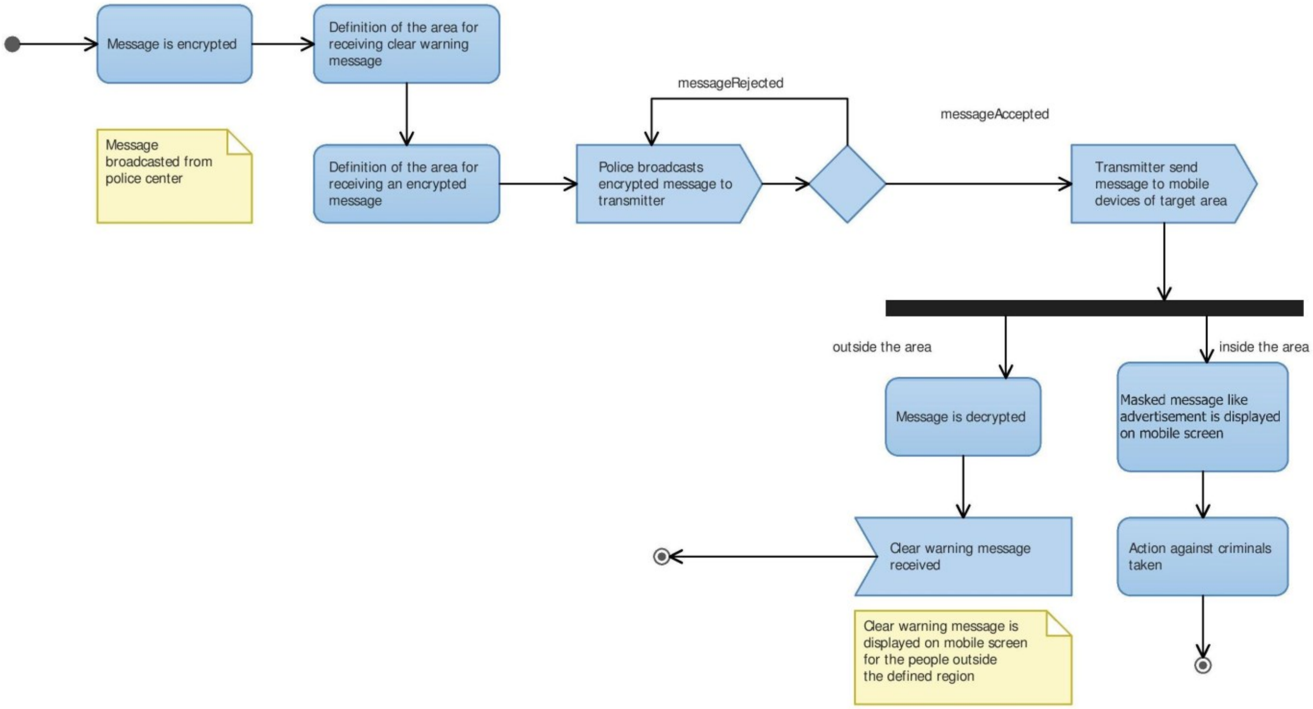
Message is encrypted
Definition of the area for receiving clear warning message
Message broadcasted from police center
Definition of the area for receiving an encrypted message
Police broadcasts encrypted message to transmitter
messageRejected
messageAccepted
Transmitter send message to mobile devices of target area
outside the area
inside the area
Message is decrypted
Masked message like advertisement is displayed on mobile screen
Clear warning message received
Action against criminals taken
Clear warning message is displayed on mobile screen for the people outside the defined region

Figure 2. Activity Diagram of the Early Warning Message Transmission Model

V. CONCLUSION AND FUTURE WORK

Positionally encrypted broadcasting system should be a future additional element to the existing concept of RADIO-HELP system, which will ameliorate its functionality. The core idea that authors will further develop is protected by a patent application - PV 2010-260 in Czech Republic (Encryption and decryption of broadcasting based on the position of listener) [13].

Throughout the creation of the model among the core issues that were discussed as possible obstacles of the execution of the process in practice and during real crisis situation, were the following: a) the limit or border between the region inside and outside the target area and its definition, b) the type of the message sent to people inside the area (encrypted) and outside the area (decrypted), since the message will be received by criminals as well and will try to escape, c) algorithmic encryption/decryption methodologies and finally, d) the technology utilized regarding the data transmission (medium of transition – transmitter, receiving devices, etc.).

The above stated topics are considered to be indispensable parts of the new functionality. This way, the combination of RADIO-HELP system and a location based encryption algorithm will formulate an innovative and useful scientific contribution in the area of location based emergency and information services.

ACKNOWLEDGMENT

This work was supported by the project No. CZ.1.07/2.2.00/28.0327 Innovation and support of doctoral study program (INDOP), financed from EU and Czech Republic funds.

REFERENCES

[1] Fire Rescue Service of the Czech Republic, “Flood situation in the Czech Republic,” [retrieved: June, 2013], Available from: http://www.hzscr.cz/clanek/flood-situation-in-the-czech-republic.aspx?q=Y2hudW09MQ%3d%3d.

[2] BBC, “Hungary battles to stem torrent of toxic sludge”, [retrieved: June, 2013], Available from: http://www.bbc.co.uk/news/world-europe-11475361.

[3] W. T. Coombs and S. J. Holanday, “The Handbook of Crisis Communications,” Chichester: Willey-Blackwell, p. 21, 2010, ISBN 978-1-4051-9441-9.

[4] Ministry of the Interior of the Czech Republic, “The terms”, [retrieved: June, 2012], Available from: http://www.mvcr.cz/clanek/mimoradna-udalost-851851.aspx.

[5] J. Skrbek, “New Possibilities of Information Services for Special Situations“, In 17 – th Interdisciplinary Information Management Talks, Proceedings (IDIMT-2009), Trauler Verlag, Linz, Sep. 2009, pp. 123-130, ISBN 978-3-85499-624-8.

[6] J. Skrbek, “Radio-Help as a Smart Early Warning and Notification System“, In Proceedings of the 55th Annual Meeting of the International Society for the Systems Sciences, 14 p, University of Hull Business School, UK, July 2011, [retrieved: June, 2013], Available from: http://journals.isss.org/index.php/proceedings55th/issue/view/11, ISSN 1999-6918.

[7] L. Scott and D. E. Denning, "Using GPS to enhance data security: Geo-Encryption," GPS World (14), April 2003, pp. 40-49.

[8] H. C. Liao and Y. H. Chao, "A New Data Encryption Algorithm Based on the Location of Mobile Users," Information Technology Journal 7 (1), 2008, pp. 63-69, ISSN 1812-5638.

[9] D. Mohapatra, and S. B. Suma, "Survey of location based wireless services," Proceedings of the International Conference on Personal Wireless Communicatons, USA, Jan. 2005, pp. 358-362. ISBN 0-7803-8964-6.

[10] J. Skrbek, "Advanced Ways and Means of Civilian Notification in Crisis Situations", In A. KOCOUREK (ed.). Proceedings of the 10th International conference: Liberec Economic Forum 1st edd., Liberec: Technical University of Liberec, 2011, pp. 419-426. ISBN 978-80-7372-755-0.

[11] iBiquity Digital, "What is HD Radio Broadcasting?", [retrieved: June, 2013], Available from: http://www. ibiquity.com/hd_radio.

[12] D. Kubát, J. Kvíz, J. Skrbek, and T. Žižka, "Distributing Emergency Traffic Information," In 20 – th Interdisciplinary Information Management Talks, Proceedings (IDIMT-2012), Johanes Kepler Universitäs, Linz, Sep. 2012, pp. 33-39, ISBN 978-3-99033-022-7.

M. Brunclík and J. Skrbek, "Encryption and decryption of broadcasting based on the position of listener," 2011, [retrieved: June, 2013], Available from: http://spisy.upv.cz/Applications/2010/PPVCZ2010_0260A3.pdf.