Secure Communication System for Emergency Services in Network Congestion Scenarios

Alexandra Rivero-García, Iván Santos-González, Candelaria Hernández Goya, Pino Caballero-Gil

Department of Computer Engineering
University of La Laguna, Tenerife, Spain
Email: {ariverog, jsantosg, mchgoya, pcaballe}@ull.edu.es

***Abstract*—Every day different events, with different risk levels, take place in cities. Emergency services are responsible for the safety of citizens and communication between emergency staff is one of the main requirements for their correct coordination and operation. A problem arises when large numbers of people are located in a particular area, which could produce saturation in traditional network infrastructures. This paper presents a low-cost model of communication to be used in this scenario. The communication system described includes an ID-Based Signcryption scheme (IBSC) that works considering the location and the public identification of emergency service workers in order to provide integrity, confidentiality, authentication and non-repudiation in a single step and in an efficient way.**

***Index Terms*—Identity Based Signcryption (IBSC); mHealth; Mobile devices; Android; Communications**

I. Introduction

This paper presents a low-cost model for communication in scenarios where network congestion is produced by massive access of users involved in emergency situations. This is a predictive scheme based on the establishment of a second communication channel that does not rely on the cloud.

The objective is to provide a suitable way of communication for emergency services (police, firefighters, medical staff, etc.) in case of events where specific alerts or activities requiring their participation (flood risk, protest march, a concert, a fire, etc.) take place. Usually, the first step is the assignment of different emergency service workers to specific areas to preserve the civil security. Figure 1 presents as an example the geolocation of three simultaneous events: a cultural event with large flow of people in green, a protest march in orange and an area with high risk of flood in blue. When an event is declared, different types of emergency service workers must be assigned to that zone. In the proposed system, the assignation of service workers is also used to generate and pre-share information among them. That is why a generic event chat, in which workers can participate via mobile phone, is included. In the event that congestion is detected in the network, the emergency mode is declared. In this specific mode, the communications will be made directly, in a peer-to-peer mode through their smartphones and without additional tools.

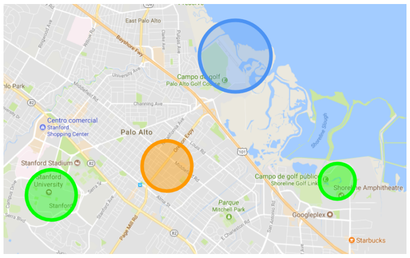

Fig. 1. Geolocation of events.

A second goal in this paper, is to guarantee the security of the shared data, thus an ID-Based Signcryption scheme (IBSC) based on the location and the public identifications of emergency service workers is used. With this cryptosystem all the shared messages will be signed and encrypted.

The majority of the communications that are currently developed within the emergency sections are carried out by radio frequency. In the proposal, communication is done through two different technologies using smartphones: Bluetooth Low Energy (BLE) [1] and via Wi-Fi Direct [2]. The features described below will be taken into account to choose the alternative. When possible the channel created by Wi-Fi Direct, due to its higher rate of speed and its greater range, will be used. Bluetooth Low Energy has a transmission rate of 25 Mbps and Wi-Fi Direct has a transmission rate of 250 Mbps. The maximum range of Bluetooth Low Energy Communication is 60 meters, while Wi-Fi Direct has a range of 200 meters. In the same range of Wi-Fi, Wi-Fi Aware improves the performance of Wi-Fi Direct. Wi-Fi Aware [3] is only available for the latest version of Android [4] and as a preview mode.

The structure of the article is described below. Section II includes a short review of publications that justify the novelty and adequacy of the proposed system. Section III deals, on the one hand, with the fundamentals of Identity-Based Cryptography since the proposal uses it to guarantee confidentiality, integrity and authenticity of the transferred information, and on the other hand deals with a presentation of a system overview. Section IV deals with the details of the communication scheme and its formal description. Some of the more common attacks in communication models are analyzed in V. Section VI ends the paper summarizing the main conclusions and contributions of the proposal.

II. Related work

Generally, communications currently deployed/used for emergency are carried out by radio frequency. It is a poor solution, because workers only can share audio in a specific frequency, effective grouping and sharing media data are not allowed. Multiple solutions based on Wi-Fi Direct and smartphones has been proposed like in [5] where there is an explanation of the potential of Wi-Fi Direct in the implementation of mobile P2P systems. This work includes some examples of the use of Wi-Fi Direct to share text messages, to disseminate information, etc. They use a middle-ware for P2P networking to distribute hash tables to search for peers. In [6], authors explain the possibility of generating opportunistic networks over Wi-Fi Direct by studying the latency at the link layer. It is an extension of [7], where multiple groups were generated. This work presents real measurements that confirm the Wi-Fi Direct's suitability for peer-to-peer systems.

There is something in common in all these systems, no security elements are proposed. Our approach differs from others in that it takes into account the distribution, assignation and location of human resources in multiple events. Furthermore, information security is addresed throughout the development of the proposed system. In [8], the authors propose the use of Wi-Fi Direct as an alternative communication system for emergency situations, but not for communication among emergency services. The main objective of the application developed there is to share the geolocation of people when they are isolated, without signal and in difficulties.

III. Proposed system

In this section, some tools are described to understand how the proposed system works. On the one hand, a cryptographic primitive is presented, which is used in the communication system and is based on identities. On the other hand, some mathematical tools are described to understand the security of the cryptographic scheme used.

A. Preliminaries

Identity based signcryption. In Identity Based Cryptosystems, the main objective is the use any string as a valid public key. These schemes often use as identifiers: email address, social security numbers, personal identifiers, etc. This kind of cryptosystem avoid problems related to certificates in public key infrastructure. Based on this idea some modifications appeared such us the Identity Based Signcryption where the main objective is to obtain a composition of an encryption scheme with a signature scheme.

Bilinear Groups. Two cycling groups $(\mathbb{G}, +)$ and $(\mathbb{G}_{\mathbb{T}}, \cdot)$ of the same prime order q are considered. P is a generator of $\mathbb{G}$ and there is a bilinear map paring $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$ which satisfies following conditions: *Bilinear*, $\forall P, Q \in \mathbb{G}$ and $\forall a, b \in \mathbb{Z}$, $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$. *Non-degenerate*, $\exists P_1, P_2 \in \mathbb{G}$ that $\hat{e}(P_1, P_2) \neq 1$. This means if P is generator of $\mathbb{G}$, then $\hat{e}(P, P)$ is a generator of $\mathbb{G}_{\mathbb{T}}$. *Computability*, there exists an algorithm to compute $\hat{e}(P, Q), \forall P, Q \in \mathbb{G}$ [9].

Elliptic Curve Discrete Logarithm Problem. Considering the cyclic group $\{\sigma, G, 2G, 3G, ...\}$ for any point G on a an elliptic curve. k is an integer where the operation kG is called a scalar multiplication. The Elliptic Curve Discrete Logarithm Problem is based on finding k given points kG and G.

B. Overview of the system

This paper presents an alternative communications system for emergency services through mobile phones in different scenarios. In order to prevent network congestion, users have to share some public information when the emergency mode is activated. This information is user's ID and it is shared through BLE using beacon mode (see Figure 2) to identify each participant. Every person has a list of identifiers (IDs) corresponding to nearby people. When an emergency service worker finds a peer sharing an ID, he/she stores this identification. Later on, IDs may be used to peer-to-peer communications.

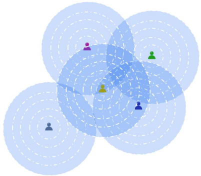

Fig. 2. Sharing identifiers through beacon mode.

The system supports two different communication modes: peer-to-peer and broadcast. In the first mode, two people can exchange information directly and bilaterally. In the broadcast mode, everyone in the affected area may receive the notification and by simply clicking on it, they can chat to help his/her colleague. Emergency staff can share text, images, audio and even videos. Security of the shared data is crucial in the proposed system. Thus, in both communication modes an ID-Based Signcryption scheme (IBSC) is used. In order to participate in the communications, each emergency service worker assigned to an area/event must also have some information. Firstly, from the central system, events are generated. Afterwards, the controller must assign different types of staff to that zone. Specific information that allows staff participation into the chat system is also provided, (see Figure 3).

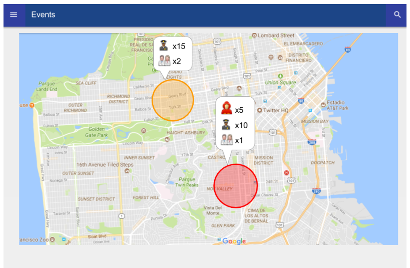

Fig. 3. Central system web application.

A unique identifier randomly generated is assigned to each event as well as the information for its geolocation. This geolocation is generated based on the focus of the event, and to prevent the generation of multiple events a range of some mills refer the same event. When a member of the emergency staff is assigned to an event, the system generates specific credentials and the keys to share data. Users may get their own location, peers's location and the area of the event from the mobile application, (see Figure 4).

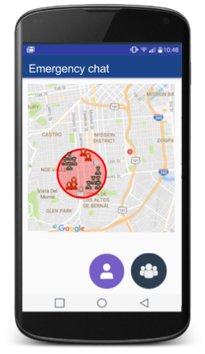

Fig. 4. Mobile application.

IV. Emergency communication scheme

As mentioned in the previous section, an ID-Based Signature scheme is used. This approach offers the advantage of simplifying management by not having to define a public key infrastructure. This kind of scheme was chosen due to its low computational complexity, efficiency in terms of memory and its usability. Emergency service staff can share information with only one person in peer-to-peer mode through an ID-Based Signcryption and with multiple users in broadcast mode through an ID-Based Multi-Receiver Signcryption Scheme. In the proposed scheme, the central server supports the Private Key Generator (PKG). It is a crucial part of the proposal, because it is the service in charge of generating emergency staff private keys. The signcryption scheme used is a combination between the ID-Based Signcryption Scheme proposed in [10] and an ID-Based Signcryption Scheme for Multiple Receivers [11]. Below, some mathematical basic elements and notation used in the system description are presented. Several hash functions are also needed: $H_1 : \{0,1\}^* \rightarrow G^*, H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*, H_3 : \mathbb{Z}_q^* \rightarrow \{0,1\}^n, H_4 : \{0,1\}^n \rightarrow \{0,1\}^{|m|}, H_5 : G \times G \times \{0,1\}^n \times Z_q^* \times Z_q^* \times ... \times Z_q^* \rightarrow Z_q^*$, where n is the size of the message. $x \overset{r}{\leftarrow} S$ stands for an element x randomly selected from a set S, $x \leftarrow y$ denotes the assignation of the value y to x and $||$ is used for concatenation. The steps needed for the signcryption scheme are the following:

SETUP: In this first step, server initializes the parameters in order to generate its own keys: master public key (mpk) and master secret key (msk). To achieve it, some private data is necessary: $k \in \mathbb{Z}$ to generate a prime q based on it, two groups $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ of order q and a bilinear pairing map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$ are selected. Next, $P \in \mathbb{G}$ is randomly selected and all the hash functions are also defined. Finally, server keys are generated $msk \overset{r}{\leftarrow} \mathbb{Z}_q^*$ and $mpk \leftarrow msk \cdot P$.

MASTER EXTRACT: In this step, the staff identification is carried out. Public key $Q_{ID} \in G$ is generated through a hash function applied on the ID, $Q_{ID} \leftarrow H_1(ID)$. Private key S_{ID}, used for communications with the server $S_{ID} \in G$, is calculated taking into account the msk, $S_{ID} \leftarrow msk \cdot Q_{ID}$. Note that key exchange between server and the staff is done using the stream cipher SNOW3G under the session key obtained through an Elliptic Curve Diffie-Hellman (ECDH).

EVENT EXTRACT: This step is required when a user is assigned to a new event. Each of the events generated has an unique identifier, $ID_e \overset{r}{\leftarrow} \mathbb{Z}_q^*$ and some location coordinates, lat and lon. In this step, the public key to this event $Q_{IDe} \in G$ is generated as: $Q_{IDe} \leftarrow H_1(ID||ID_e||lat||lon)$. Then, the secret key to this event $S_{IDe} \leftarrow msk \cdot Q_{IDe}$.

EVENT SINGLE SIGNCRYPTION: All the messages $m \in \{0,1\}^n$ will be encrypted and signed. The receiver's public key is generated taking into account his/her identification and the pre-shared data (ID_e, lat and lon): $Q_{IDe_b} \leftarrow H_1(ID_b||ID_e||lat||lon)$. Then, some operations are developed giving as result σ (a t-uple of three components: c, T, U). T is generated as $x \overset{r}{\leftarrow} \mathbb{Z}_q^*$ and $T \leftarrow x \cdot P$. Then the signature using sender's private key (S_{IDe_a}) is in U. It is obtained as follows $r \leftarrow H_2(T||m)$, $W \leftarrow x \cdot mpk$ and $U \leftarrow r \cdot S_{IDe_a} + W$. Finally the encrypted message is in c, and it is generated as shown below $y \leftarrow \hat{e}(W, Q_{IDe_b})$, $k \leftarrow H_3(y)$, $c \leftarrow k \oplus m$.

EVENT BROADCAST SIGNCRYPTION: In the broadcast mode there are n receivers, so the sender is identified by IDe_a and the receivers by $IDe_1, IDe_2, ..., IDe_n$. All the broadcast messages $m \in \{0,1\}^n$ will be encrypted and signed. The sender's public key is generated as bellows: $Q_{IDe_a} \leftarrow H_1(ID_a||ID_e||lat||lon)$. Then some operations are developed giving as result σ (a t-uple of components: $c, T, U, V, W, X, a_0, ...a_n - 1$), then the sender selects some random numbers $r \overset{r}{\leftarrow} \mathbb{Z}_q^*$, $r' \overset{r}{\leftarrow} \mathbb{Z}_q^*$, $s \overset{r}{\leftarrow} \mathbb{Z}_q^*$ and $p \overset{r}{\leftarrow} \mathbb{Z}_q^*$ and then, it operates $T \leftarrow r \cdot Q_{IDe_a}$, $U \leftarrow r \cdot P$, $X \leftarrow r' \cdot T$, $J \leftarrow r' \cdot mpk$. The receivers' public keys are generated taking into account all the identifications $ID_1, ID_2, ..., ID_n$, as follows: $f(x) = \prod_{i=0}^{n}(x - v_i) + p(modq) = a_0 + a_1 x + ... + a_{n-1}x^{n-1} + x^n$ with $Qe_i \leftarrow H_1(ID_i||ID_e||lat||lon)$, $y_i \leftarrow \hat{e}(Q_i, J)$ and $v_i \leftarrow H_2(y_i)$. Then it calculates $V \leftarrow s \cdot H(p)$, the key k as $k \leftarrow H(s)$ and the encrypted message c as $c \leftarrow k \oplus m$. Finally an authenticator h is generated as $h \leftarrow H_5(c, X, U, V, a_0, a_1, ..., a_{n-1})$ and $W \leftarrow (r' + h)r \cdot S_{ID_a}$.

EVENT SINGLE UNSIGNCRYPTION: First of all the sender's public key is generated taking into account IDe_a and the pre-shared information as $Q_{ID_a} \leftarrow H_1(IDe_a||ID_e||lat||lon_e)$. Then σ is parse as (c, T, U). If everything is right, the message $m \in \{0,1\}^n$ is returned. Otherwise, if there are some problems in the signature or in the encryption of m, $\perp$ is returned. The verification is : $\hat{e}(U, P) == \hat{e}(Q_{IDe_a}, mpk)^r \cdot \hat{e}(T, mpk)$ Thus, the user calculates $y \leftarrow \hat{e}(S_{IDe_b}, T)$, $k \leftarrow y$, $m \leftarrow k \oplus c$ and $r \leftarrow H_2(T||m)$.

MULTIPLE RECEIVER UNSIGNCRYPTION: In this step, two verifications are carried out but first of all

σ is parse as $c, T, U, V, W, X, a_0, ...a_n - 1$ and $h \leftarrow H_5(c, X, U, V, a_0, a_1, ..., a_{n-1})$. The first verification is the public verification to check that the ciphertext is valid: $\hat{e}(W, P) == \hat{e}(X + hT, mpk)$ Otherwise, the ciphertext has been damaged or it is invalid and $\perp$ is returned. The second verification is: $\hat{e}(W, Qe_i) == \hat{e}(X + hT, S_{IDe_i})$ It is to check if ID_i is one of the receivers chosen by the sender and the ciphertext is valid. Otherwise, the receiver shall quit the decryption process and $\perp$ is returned. To generate the message some operations are generated: $y_i \leftarrow \hat{e}(S_{IDe_b}, U)$, $v_i \leftarrow H_2(y_i)$, $p \leftarrow f(v_i)$, $s \leftarrow V \oplus H_3(p)$, $k \leftarrow H_4(s)$ and $m \leftarrow k \oplus c$.

V. Prototype analysis

A system prototype has been developed. It includes a web application and a mobile application to improve communication between emergency services in extreme situations. Security is one of the priorities that is why the system provides protection against different attacks. On the one hand, Denial of Service (DoS) attacks related to make multiple requests are restricted because only requests associated with a number of legitimate members of emergency services take effect. On the other hand, the typically "Man in the Middle" attack which conveys a successful authentication to the server with a legitimate identifier is very improbable, because once the corresponding user private key is assigned to the server further requests of this kind will be not attended. Impersonation will be easily detectable since the number of members who can make requests to the server is limited to those who are working at the time of the request.

An analysis of efficiency related to the technologies coverage, their range and their transmission efficiency was developed. A beta prototype has been also implemented with Wi-Fi Aware but in the preview mode of the technology. An Android application has been developed to share information between users. The implementation of the security has been developed with the generation of some random events on a map and with the assignation of users to events manually.

Note that the proposed prototype does not need a communication with the PKG, but just for the initialization where the generation of keys is performed in the Event Extract step. Afterwards, users can share messages with their own keys and with the pre-shared information related to the event. This eliminates the problem of saturated communication networks because an alternative scheme has been displayed with direct communications that do not need a central server.

VI. Conclusions and future work

In this paper a low-cost communication model has been presented as an alternative communication system for situations where network congestion was detected. The tool has been proposed like a combination of a web application, that manages all the emergency services and events, and a mobile application with an ubiquitous Wi-Fi Direct chat. Communication security was based on the use of a public key cryptosystem and BLE in beacon mode. Emergency services were able to know, with the mobile application, where the event was located and where they must deployed, as well as peers location. The system generated automatically the pre-shared data depending on the event to which the worker has been assigned; the main objective was that emergency workers was able to share information among them when different events saturate the network. The prototype has been developed like an emergency support tool to contact peers through a chat. An ID-Based Signcryption has been used to protect integrity, confidentiality, authentication and non-repudiation in the communications. Specifically, emergency service shared information with only one person in peer-to-peer mode and with multiple users in broadcast mode.

As future work, more functionalities will be added to the server, such as statistics, private chats based on roles, etc. The improvement of communication technologies is a must. A beta prototype has been implemented with Wi-Fi Aware that is available only in Android 8 and in the preview mode of the technology. The addition of LTE-Direct depends on the Native Development Kit (NDK), because right now this code is private.

Acknowledgment

Research supported by TESIS2015010102, TESIS-2015010106 and by the Spanish Ministry of Economy and Competitiveness, the European FEDER Fund, and the CajaCanarias Foundation, under Projects TEC2014-54110-R, RTC-2014-1648-8, MTM2015-69138-REDT and DIG02-INSITU.

References

[1] N. K. Gupta, *Inside Bluetooth low energy*. Artech House, 2016.

[2] W. Shen, B. Yin, X. Cao, L. X. Cai, and Y. Cheng, "Secure device-to-device communications over wifi direct," *IEEE Network*, vol. 30, no. 5, pp. 4–9, 2016.

[3] B. N. Schilit, A. LaMarca, G. Borriello, W. G. Griswold, D. McDonald, E. Lazowska, A. Balachandran, J. Hong, and V. Iverson, "Challenge: Ubiquitous location-aware computing and the place lab initiative," in *Proceedings of the 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots*. ACM, 2003, pp. 29–35.

[4] O. Android, "Android," *Retrieved February*, vol. 24, p. 2011, 2011.

[5] R. Motta and J. Pasquale, "Wireless p2p: Problem or opportunity?" in *Proceedings of the Second IARIA Conference on Advances in P2P Systems*, 2010, pp. 32–37.

[6] M. Conti, F. Delmastro, G. Minutiello, and R. Paris, "Experimenting opportunistic networks with wifi direct," in *Wireless Days (WD), 2013 IFIP*. IEEE, 2013, pp. 1–6.

[7] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, "Device-to-device communications with wi-fi direct: overview and experimentation," *IEEE wireless communications*, vol. 20, no. 3, pp. 96–104, 2013.

[8] I. Santos-González, A. Rivero-García, P. Caballero-Gil, and C. Hernández-Goya, "Alternative communication system for emergency situations." in *WEBIST (2)*, 2014, pp. 397–402.

[9] J. Groth and A. Sahai, "Efficient non-interactive proof systems for bilinear groups," *Advances in Cryptology–EUROCRYPT 2008*, pp. 415–432, 2008.

[10] J. Malone-Lee, "Identity-based signcryption." *IACR Cryptology ePrint Archive*, vol. 2002, p. 98, 2002.

[11] S. S. D. Selvi, S. S. Vivek, R. Srinivasan, and P. R. Chandrasekaran, "An efficient identity-based signcryption scheme for multiple receivers," Cryptology ePrint Archive, Report 2008/341, 2008, https://eprint.iacr.org/2008/341.