IBSC System for Victims Management in Emergency Scenarios

Alexandra Rivero-García, Iván Santos-González, Candelaria Hernández-Goya and Pino Caballero-Gil
Departamento de Ingeniería Informática y de Sistemas, Universidad de La Laguna, Tenerife, Spain

Keywords: Identity-based Signcryption, Keyed-Hash Message Authentication Code, Security, Triage, Emergency.

Abstract: This work describes an optimized system designed to help the greatest number of injured people in emergency situations, using the shortest possible time and cost. It is composed of a mobile application (assigned to medical staff and helpers), a web service and Near Field Communication wristbands assigned to victims. The mobile application is devoted to providing medical staff with the geolocation of victims as well as with an assistant indicating the best route to follow in order to take care of them based on the severity of their conditions and based on a triage method. Resolution of the routes is solved based on a classical problem, a Travelling Salesman Problem, using a k-parition algorithm to divide the huge number of victims in different clusters. Thus, each doctor has a specific area to assist victims. Besides, doctors can use a functionality of the application to contact their peers through a video call when additional help is needed. The proposal combines an keyed-Hash Message Authentication Code scheme to protect Near Field Communication tags and an IDentity-Based Cryptosystem to the wireless communication. Specifically an IDentity-Based Signcryption is used for communication confidentiality, authenticity and integrity, both among peers, and between server and medical staff.

1 INTRODUCTION

The communication technologies used in smartphones and the power of these devices can help in many complex scenarios. Smartphones are used to support different daily tasks, their small size and high performance is a huge advantage. This paper presents a platform for improving logistics of medical staff in emergency situations in a distributed way. In particular, it is based on data obtained from a triage application developed in (Rivero-Garcıa et al., 2014), where a mobile system for victim classification in emergency situations was implemented.

The definition of triage can be described as follows. A simple, complete, objective and fast process to obtain an initial clinical assessment of people with the objective of evaluating their immediate survival capacities and prioritizing them according their severity is a triage. In order to achieve the classification, all triage systems distinguish two steps. The first triage or simple triage is used for the generation of a classification based on the severity of injuries of the victims evaluating their survival skills in some seconds. The second triage is where medical staff analyses each patient's state: bruises, wounds and injuries. Specifically, in this work, Simple Triage and Rapid Treatment Algorithm (START) method is used as first triage. Its output is the victim's classification based on coloured tags, where each colour defines the priority of the victim: black, dead or irrecoverable victims; red, victims requiring immediate care; yellow, victims requiring urgent care but who can wait for treatment from half an hour to one hour; green, victims who are not seriously injured. They can wait for treatment more than an hour. Here the use of Near Field Communication (NFC) is proposed to deal with the triage result. NFC stickers are used to save triage results based on the generation of a keyed-Hash Message Authentication Code (HMAC) scheme. Furthermore, the route to attend victims for each doctor is shown through a map in their smartphones based on the priorities of victims and they can share information peer-to-peer with their colleagues in the affected area. All these communications are protected through an IDentity-based (ID-based) cryptography, specifically a ID-Based Signcryption scheme (IBSC).

This work is organized as follows. Section 2 provides some preliminaries while Section 3 gives a global view of the proposal. Then, Section 4 sketches the system that is used to make decisions. The topic of victim identification through NFC tags and HMAC schemes is dealt in Section 5. The protection of security related to the medical staff through an IBSC scheme is proposed in Section 6. A brief security ana-

Rivero-García, A., Santos-González, I., Hernández-Goya, C. and Caballero-Gil, P.
IBSC System for Victims Management in Emergency Scenarios.
DOI: 10.5220/0006298702760283
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 276-283
ISBN: 978-989-758-245-5

lysis is provided in Section 7. Finally, a few conclusions and future works close the paper.

2 PRELIMINARIES

There are still some weaknesses in emergencies management. The integration of new technologies into emergency situations management and medical care has allowed the development of tools that help to the coordination between medical staff in emergency scenarios. There are different proposals designed to help to find missing persons after a large-scale disaster. Such as People Locator and ReUnite (of Medicine at NIH, 2017), Google person finder (Google, 2017) and Safety Check of Facebook (Facebook, 2017). All these systems try to verify and share the status of people after some disaster, specifically the proposal of Facebook share all the information with the victim's friends in this social network.

Some organizations are working to provide different solutions related to emergency situations. One of then is Sahana foundation (Foundation, 2017) project aims to provide a set of modular, web-based disaster management applications. This project includes tools for synchronization between multiple instances: a Missing Person Registry, Request and Pledge Management System and Volunteer coordination. Since this proposal is a web-based framework, it has the problem of relying on communication to the centralized web-server, and thus cannot take advantage of mobile nodes. There are no solutions to the identification of victims. The unique identification of affected people is a requirement for any emergency triage. Barcodes are a possibility because they facilitate mechanical reading (Neuenschwander et al., 2003). Barcodes are cheap and easy to create, they can be generated just using a standard printer. But in an emergency situation having a printer in the affected zone is not realistic. Radio Frequency IDentification (RFID) is a very useful technology for victim identification as it is explained in (Inoue et al., 2006) and in (Baracoda, 2017). Two types of tags exists, passive tags, that use the energy received from the reader to send the identifier, and active tags, that include a battery to increase its distance range. The problem of this kind of communication is that a RFID reader is needed and no security tools were provided. In (Gao et al., 2007) a specific triage tag technology is proposed. These electronic triage tags use noninvasive biomedical sensors to continuously monitor the vital signs of a patient and deliver pertinent information to first responders. These are not triage tag for emergency situations.

The use of NFC (Near Field Communication)(Want, 2011a) is one of the bases of the proposed system, specifically NFC stickers, for automatic patient identification. Unlike other technologies as RFID (Zou et al., 2014), Bluetooth or Wi-Fi (Lee et al., 2007), NFC is not oriented to the continuous data transmission. It is necessary a temporally contact between the devices that interact to allow the exchange of information in a quick and timely way. Although, at first, the distance factor for transmitting information may seem a limitation it is actually the key in this technology. The need for proximity between devices limits the types of attacks to develop. Besides, not requiring pairing between devices facilitates its use by health staff. NFC devices may operate in two different modes. On the one hand, in the active mode each device generates its own electromagnetic field (emulating the communication paradigm peer-to-peer). On the other hand, in the passive mode one device generates the electromagnetic field with its own power supply. In this way, it enables that other device starts the connection taking energy from the field generated to power its circuit. Then the passive device generates the response signal and transfers the data. This mode of operation matches with the RFID communication model and it is the one used in this proposal.

3 GLOBAL VIEW

The main objective of the proposal is to generate a tool to save as many time as possible in emergency situations. Therefore, doctors have a map in their mobile phones that helps them in every moment to decide the route to patients. This route is based on the severity of the injuries. Thus, collisions of doctors to assist the same patient are avoided and decisions are taken based on priority.

Two stages in the route generation are made. The first one consists in the evaluation of the affected area applying START triage method to obtain a victims' classification based on coloured tags. This is generated by the first aid team, where there are medical staff, firefighters or even rescue services.

As we mentioned previously, each colour defines the priority of the victim: black, dead or irrecoverable victims; red, victims requiring immediate care; yellow, victims requiring urgent care but who can wait for treatment from half an hour to one hour; green, victims who are not seriously injured. They can wait for treatment more than an hour. This colour result is stored on tags. In this case NFC (Want, 2011b) tags, specifically NFC stickers are used to save the triage result. Note the proposed work uses NFC stickers but multiple kind of NFC tags can be used, depending on the emergency and the victims state. Each triage has a location in the central server. At the end of this step the system has a map with the location of each victim and their triage like in figure1.

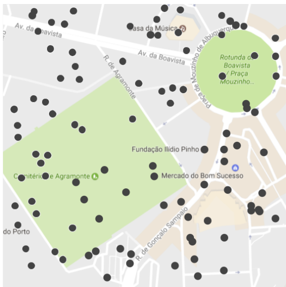


Figure 1: Victims' location.

The second stage is based on the victim's attention taking into account the results of the triage priorities. In this step the victims' locations given by the first triage is essential being the starting point. A graph of each colour is generated based on the victim's location in a map. Victims represent nodes and the routes to reach them are de edges. Each edge has a cost. This cost is the distance between two nodes calculated through the Haversine Formula (Knox, 2015), where $cos_{\gamma_{AB\Delta\lambda}} = cos(\gamma_A) \cdot cos(\gamma_B) \cdot hvsin(\Delta\lambda)$, then:

$$hvsin(\frac{d}{R}) = hvsin(\gamma_A - \gamma_B) + cos_{\gamma_{AB\Delta\lambda}} \qquad (1)$$

Where hvsin is the haversine function:

$$hvsin(\theta) = sen^2(\frac{\theta}{2}) = \frac{1 - cos(\theta)}{2} \qquad (2)$$

d is the distance between two points (over the bigger circle of the sphere), R is the sphere radio, in our case the Earths radio, γ_A is the latitude of the point A, γ_B is the latitude of the point B and $\Delta\lambda$ is the difference of the longitudes.

Finally, if $sen_{\gamma_{AB}} = sen(\gamma_A) \cdot sen(\gamma_B)$ and $cos_{\gamma_{AB}} = cos(\gamma_A) \cdot cos(\gamma_B)$, the distance ($d$) is:

$$d(A,B) = R * arccos(sen_{\gamma_{AB}} + cos_{\gamma_{AB}} * cos(\Delta\lambda)) \qquad (3)$$

All information related to the patients who must be attended by a doctor is done through a mobile application. It indicates to the medical staff through a map his/her current location and the next patient to assist.

The application has enabled a feature called "emergency support". With this function when a doctor or nurse requires additional help from peers he/she can activate this mode. When they activate this feature all health personnel in the affected area receives the notification and simply by clicking on it, they can start a video call or a chat to help his/her colleague. This functionality was designed to support healthcare workers and improve the use of time in transfers between patients. Note that this feature opens a communication channel between two partners through a video streaming. Due to the high amount of information exchanged the connection will take place by Long Term Evolution (LTE)(Sesia et al., 2009), specifically LTE-Direct to ensure adequate and secure communication between nodes that connect.

In the moment in which a doctor has just treat a victim, he/she can take his/her mobile and read the tag, mark the point as completed and check next victim status. When the doctor arrives to the location of the new victim, the node is automatically marked on the map as being in the care process but he/she can read the sticker to be sure of the authenticity of the node. The period devoted to reach a new node is called "travelling time". Doctors can receive notifications called "emergency support" when they are in this "travelling time" to avoid constant notifications that may mislead the staff in the middle of an assistance.

4 DECISION-MAKING SYSTEM

First of all, in the generation of doctors' routes, an undirected graph is created from the points defined during the triage. There are as many points as patients on the map, these are the vertices of our graph. The edges will be defined undirected between the vertices. This distance between points will be the cost of the edge. The system generates one graph for each triage colour, the main objective is treating patients based on their injuries. First of all, the patients with red triage are care, then patients with yellow triage and finally the ones with green triage. Once each graph is generated, the amount of resources and the place where they are needed. In this case resources are doctors (number of doctors #d) that will assist patients. Their position at all time is known. Specifically a graph based on the Delaunay Triangulation (de Berg et al., 2008) is created (as in figure 2) .

Initially, the system divides into clusters the red graph. At the end, there are as many subgraphs as doctors in the emergency area. Specifically our system generates a $k - partition$ based on (Hespanha, 2004), where k is the number of doctors (#d). The system assigns to each doctor, depending on the location, the node that is the highest priority and closest to the coloration performed. That is, the nearest doctor

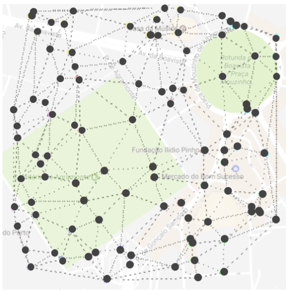


Figure 2: Graph based on Delaunay Triangulation.

is distributed for each partition, excluding the doctors already assigned. This is a quick solution for distributing to doctors in different areas. If a new node is generated, the system automatically add it to the nearest cluster, and a new doctor's route is recalculated.

Definition 1. *k-partition. Consider $G = (V,E)$ as an undirected graph with the set V as vertex and the set E as edges and where the edge cost function is $c : E \to [0,\infty)$. A $k-partition$ of V is a collection $P = \{V_1,V_2,...,V_k\}$ of k disjoint subsets of V, whose union equals V. The cost associated with P is defined by:*

$$C(P) = \sum_{i \neq j} \sum_{(v,\bar{v}) \in E v \in V_i, \bar{v} \in j} \bar{c}(v,\bar{v})$$

The $l-bounded$ Graph Partitioning $(l-GP)$ problem is based on finding a $k-partition$ P that minimizes $C(P)$, with no more than l vertices in each partition. The problem is based on the $MAXk-CUT$ problem (de Sousa et al., 2016) that find a partition for F that maximizes the reward for a edge-reward given as $r : V \times V \to [0,\infty)$, where $r(v,\bar{v}) = r(\bar{v},v), \forall v,\bar{v} \in V$. We considered a variation of this problem called Hypergraph Max k-CUT (HMkC) *problem (Ageev and Sviridenko, 2000) with the sizes of parts given and for a set of k integers $s_1,s_2,...,s_k$ adds the constraint $|V_i| = s_i, \forall i$.*

Note if there are red nodes (number of red nodes $\#r$) the other colours are not considered. When these victims are attended the yellow nodes(y) are taken into account and finally green nodes(g).

When the graph is divided as in figure (figure 3) the system assign one doctor for each zone. Then the system analyses the path of each subgraph. This is the problem known as the Travelling Salesman Problem (TSP) (Hoffman et al., 2013) and we solve this through a Genetic Algorithm (Mudaliar and Modi, 2013).

These methods are adaptive and may be used to solve optimisation and search problems. They are inspired by the behaviour of the species to evolve and belong to the group of genetic algorithms.

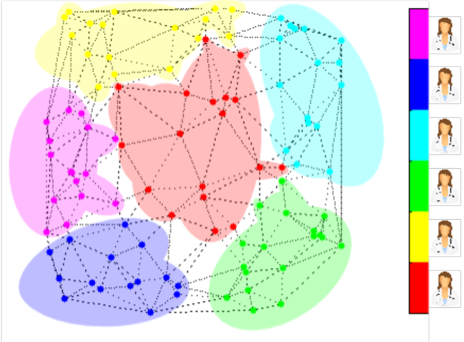
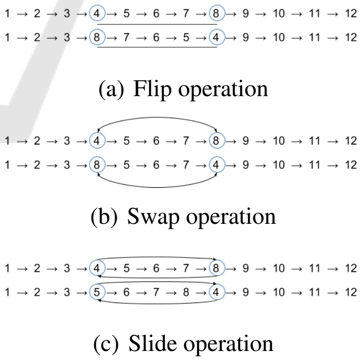


Figure 3: k-Partition graph.

Populations are made up of different individuals. In the problem posed here when talking about individuals we refer to victims / possible routes that can be obtained.

A simulation has been carried out in order to validate the use of this approach to build the routes. For each subgraph a population of 100 individuals is randomly generated. A selection of the best four individuals (the lowest cost route) is made. From them the parts that routes have in common are selected as parents for generating the new population and children are generated by permuting the order of the part that does not match.

Once the new population is generated, random mutations based on three different operations as shown in the figure 4 are made. This iteration is repeated 1000 times before getting the final result.



(a) Flip operation

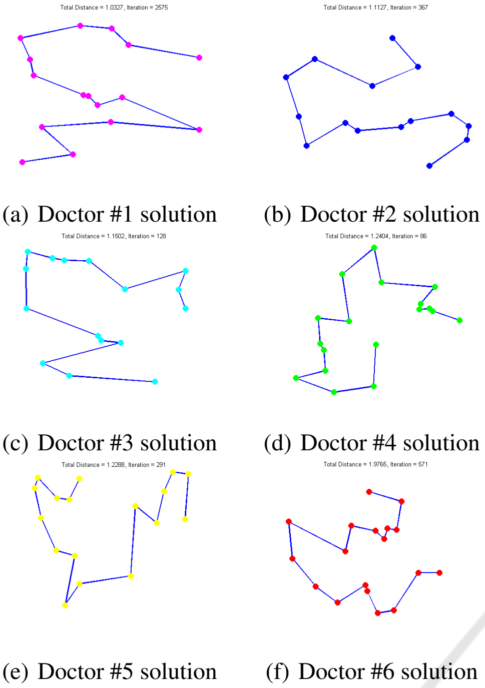
(b) Swap operation

(c) Slide operation

Figure 4: Operations to generate mutations.

Finally, once the genetic algorithm is applied to each subgraph obtained after the partition, the different routes for each doctor are obtained, such as it is illustrated in figure 5.

The number of iterations and the population size was chosen based on the results of time and costs we obtained in different simulations. These values are an approximation that can be adjusted at any time. Thus, a graph of routes is generated for each doctor,



(a) Doctor #1 solution (b) Doctor #2 solution

(c) Doctor #3 solution (d) Doctor #4 solution

(e) Doctor #5 solution (f) Doctor #6 solution

Figure 5: Routes of Doctors.

based on the combination of different subgraphs that are produced with patients of the same priority level. At the time of generating the graph of the following categories (colours), the last vertex added to the previous graph is the starting point of the new graph. This generation of separated subgraphs is based on the regulations when applying triage schemes because patients may be attended in order depending of the severity of injuries. If a patient walks, and a medical staff re-triages her/him, the system updates the information and the mobile application updates the NFC tag if it is necessary.

The incorporation of new medical staff or new casualties does not cause any problems or additional cost. If more nodes are added to the graph the doctors' routes are updated paying attention to the new characteristics of the affected area. The routes will be reseted and each doctor can continue his/her work without worrying about such distractions. Given a constraint, doctors who are in the "travelling time" will not receive the route update until he/she has attend next victim, this will the starting point of the route this is never stored in the NFC tag.

5 VICTIMS IDENTIFICATION: NFC TAGS AND HMAC SCHEME

A member of the medical staff is who assign NFC tags to victims in the system proposed. All of these tags contain the result of the triage, that is to say the colour of the triage classification, jointly with the location and the result of a HMAC generated by the server, the physical identifier of the NFC tag (idTag) and some server data explained later in the paper. The stored information will serve as patient identification both in for triage as well as in the medical records generated later on at the hospital. If some data is gathered the system sends it to the server

The use of smartphones helps in the identification of patients through NFC stickers by using phones as NFC readers. Apart of this, devices send the physical tag identifier to the server. In the server, two 64 bytes arrays are generated (Smart, 2016). They are *ipad* and *opad* arrays, and they have default values defined at the initialization stage. The new arrays are generated through a XOR operation combining the previous values and the Master Secret Key (msk). The results are *ipadkey* y *opadkey* arrays (figure 6). After that, the HMAC value is generated with the physical tag identifier and the triage colour result T_{result} (it is a letter for each colour: B, black; R, red; Y, yellow and G, green), so the system applies a hash function to the concatenation of these fields and the *ipadkey*. The output of this hash concatenated with the *opadkey* is the input to another hash function.

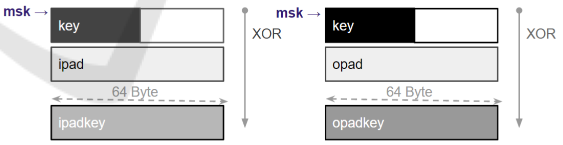


Figure 6: HMAC Keys Generation.

The global function may be described as:

$$H1 = HASH(ipadkey||idTag||T_{result})$$

$$HMAC(Tid, msk) = HASH((opadkey)||H1)$$

The hash function chosen for the implementation is a $SHA3_{512}$. The final output will be the identifier that the will be saved in the NFC sticker tag, as you can see in figure 7.

When a doctor or a member of the medical staff want to access to the triage result of a patient, in the affected zone, he/she has to read the NFC sticker through the mobile application which sends the data of the physical tag identifier and HMAC to the server. The server is who verifies the authenticity of the tag

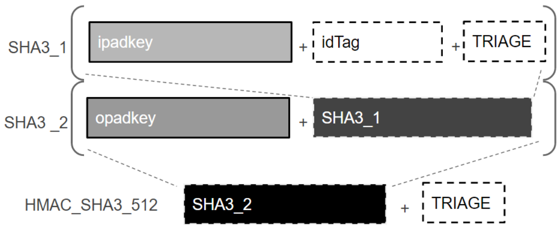


Figure 7: HMAC Hash Operation.

and generates a new node. The doctors can see all the nodes in the mobile phone, specifically the nodes on his/her routes.

6 MEDICAL STAFF SECURITY: IBSC SCHEME

Different communications modes are supported related with medical staff. On the one hand, the communication with the server (to check NFC tags authenticity and synchronizing routes) and, on the other hand the communication between them (video-calls and chats). Authentication against the server and peers and integrity of shared data is included. In both communication modes an ID-Based Signcryption scheme (IBSC) is used in order to achieve secure communications. This complex cryptosystem is a combination of ID-Based Encryption (IBE) and ID-Based Signature (IBS) that provides private and authenticated delivery of information between two parties in an efficient way with a composition of an encryption scheme with a signature scheme (Boyen, 2010). This approach offers the advantage of simplifying management by not having to define a public key infrastructure. This type of scheme was chosen due to its low computational complexity, efficiency in terms of memory and its usability.

A crucial part of the proposal is a Private Key Generator (PKG), a server in charge of generating health staff private keys. The identifier of medical staff is the number of registered medical practitioners and for nurses the same (*ID*). Next, we describe the mathematical basic tools used as well as the notation included in their description.

Definition 2. *Considering two cycling groups* $(G,+)$ *and* $(V,\cdot)$ *of the same prime order q. Pis a generator of G and there is a bilinear map paring* $\hat{e}: G\times G \to V$ *satisfying the following conditions:*

- *Bilinear:* $\forall P,Q \in G$ *and* $\forall a,b \in \mathbb{Z}$, $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$
- *Non-degenerate:* $\exists P_1,P_2 \in G$ *that* $\hat{e}(P_1,P_2) \neq 1$. *This means if P is generator of G, then* $\hat{e}(P,P)$ *is a generator of Q.*
- *Computability: there exists an algorithm to compute* $\hat{e}(P,Q), \forall P,Q \in G$

Some hash functions denoted as follows are also needed: $H_1 : \{0,1\}^* \to G^*, H_2 : \{0,1\}^* \to \mathbb{Z}_q^*, H_3 : \mathbb{Z}_q^* \to \{0,1\}^n$, where the size of the message is defined by n. The signcryption scheme used is the ID-Based Signcryption Scheme (IDSC) proposed in (Malone-Lee, 2002). Next we describe some basic notation used: $x \xleftarrow{r} S$ 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:** The initial parameters are established and the server generates the master public key (*mpk*) and the master secret key (*msk*). For that a prime q based on some private data $k \in \mathbb{Z}$, two groups G and V of order q and a bilinear pairing map $\hat{e}: G\times G \to V$ are selected. $P \in G$ is selected randomly and the hash functions H_1, H_2 and H_3 are also chosen.

$$msk \xleftarrow{r} \mathbb{Z}_q^*$$
$$mpk \leftarrow msk \cdot P$$

- **EXTRACT (*ID*):** In this step, the secret key for each member of the medical staff based on their ID is generated. The public key $Q_{ID} \in G$ and the secret key $S_{ID} \in G$ are calculated taking into account the *msk*. It should be pointed out that this key exchange between server and the doctor is performed using the stream cipher SNOW3G (Santos-González et al., 2014) under the session key obtained through an Elliptic Curve Diffie-Hellman (ECDH)(Bos et al., 2014). the safety of following connections as you can see in figure **??**.

$$Q_{ID} \leftarrow H_1(ID)$$
$$S_{ID} \leftarrow msk \cdot Q_{ID}$$

- **SIGNCRYPTION (**S_{ID_a}**,** ID_b**,** m**):** All the messages $m \in \{0,1\}^n$ will be encrypted and signed. The receiver's public key is generated taking into account ID_b and then the message is signed with S_{ID_a} and encrypted with Q_{ID_b} giving as result σ (a t-uple of three components: c, T, U).

$$Q_{ID_b} \leftarrow H_1(ID_b)$$
$$x \xleftarrow{r} \mathbb{Z}_q^*$$
$$T \leftarrow x \cdot P$$

$$r \leftarrow H_2(T||m)$$
$$W \leftarrow x \cdot mpk$$
$$U \leftarrow r \cdot S_{ID_a} + W$$
$$y \leftarrow \hat{e}(W, Q_{ID_b})$$
$$k \leftarrow H_3(y)$$
$$c \leftarrow k \oplus m$$
$$\sigma \leftarrow (c, T, U)$$

- **UNSIGNCRYPTION** (**ID_a, S_{ID_b}, σ**)**:** 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 sender's public key is generated taking into account ID_a and then the message is unencrypted with S_{ID_b}.

$$Q_{ID_a} \leftarrow H_1(ID_a)$$
$$split \quad \sigma \quad as \quad (c, T, U)$$
$$y \leftarrow \hat{e}(S_{ID_b}, T)$$
$$k \leftarrow y$$
$$m \leftarrow k \oplus c$$
$$r \leftarrow H_2(T||m)$$

Verification:

$$\hat{e}(U, P) == \hat{e}(Q_{ID_a}, mpk)^r \cdot \hat{e}(T, mpk)$$

Note: if the verification is successful m is returned, otherwise $\perp$ is returned.

7 SECURITY ANALYSIS

The proposed scheme provides protection against different attacks. In this sections some of them are presented. On the one hand, a spoofing attack and/or cloning of the card will be hardly successful since it would involve the generation of the HMAC described taking into account the master key of the server and the ID card. Even if an outsider obtains this information, it should be noted that the physical identifier of a NFC tag is unique to each element. On the other hand, if someone emulate a NFC card from an Android device, in this operating system, the emulated device goes from being passive to being active. So the attack would be detected since the application has the restriction that only read NFC tags that are passive. At the time of its implementation in Android are different and completely distinguishable communications.

Attacks related to make multiple requests to the server, called Denial of Service (DoS) attack, are restricted because only requests associated with a number of legitimate members of the medical staff will take effect. Once the corresponding private key is assigned, more requests of this kind will be not attended.

Finally, the typically "Man in the Middle" attack which conveys a successful authentication to the server with an identifier of legitimate members of the medical staff is improbable. This false identification would be easily detectable because the number of members who can make requests to the server is limited to those who are working at the time of the request. This authentication is one of the most important points on every cloud computing system based on mobile phones (Alizadeh et al., 2016).

8 CONCLUSIONS AND FUTURE WORK

In this work, a system has been presented to may to improve logistics and attention of casualties in extreme situations. The priority is to serve the greatest number of injuries using the shortest possible time and cost. The tool consists on a mobile application, NFC tags and a web service. The mobile application helps health staff to know in every moment the position of the victim and where they must go. Specifically the system create a graph based on the Delaunay Triangulation and uses a $k - partition$ to divide it in clusters. Different subgraphs are obtained, as many ones as doctors in the emergency area. When the graph is divided the system assign one doctor for each zone. Then the system analyses the path of each subgraph through a Genetic Algorithm to solve it like a TSP. The system has an "emergency support" tool to contact peers through a video call when doctors require additional support. Data security is a key objective, so for this reason a HMAC scheme is used to protect NFC tags and an ID-Based Signcryption is used for the communications. A first approach has been implemented in Android and Nodejs with NFC tags. More functionalities can be added to the server, such as statistics, a real-time map with events, etc. Thus, this task is part of a work in progress.

ACKNOWLEDGEMENTS

Research supported by TESIS2015010102, TESIS2015010106, RTC-2014-1648-8, TEC2014-

54110-R, MTM-2015-69138-REDT and DIG02-INSITU.

REFERENCES

Ageev, A. A. and Sviridenko, M. I. (2000). An approximation algorithm for hypergraph max k-cut with given sizes of parts. In *Algorithms-ESA 2000*, pages 32–41. Springer.

Alizadeh, M., Abolfazli, S., Zamani, M., Baharun, S., and Sakurai, K. (2016). Authentication in mobile cloud computing: A survey. *Journal of Network and Computer Applications*, 61:59–80.

Baracoda (2017). Idbluean efficient way to add rfid reader/encoder to bluetooth pda and mobile phones. Available online: http://www.baracoda.com (accessed on 15 February 2017).

Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., and Wustrow, E. (2014). Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security*, pages 157–175. Springer.

Boyen, X. (2010). *Identity-based signcryption*. Springer.

de Berg, M., Cheong, O., van Kreveld, M., and Overmars, M. (2008). Delaunay triangulations. *Computational Geometry: Algorithms and Applications*, pages 191–218.

de Sousa, V. J. R., Anjos, M. F., and Le Digabel, S. (2016). Computational study of valid inequalities for the maximum k-cut problem.

Facebook (2017). Facebook safety check. Available online: https://www.facebook.com/about/safetycheck/ (accessed on 15 February 2017).

Foundation, S. (2017). Open source disaster management software. Available online: https://sahanafoundation.org/ (accessed on 15 February 2017).

Gao, T., Massey, T., Selavo, L., Crawford, D., Chen, B.-r., Lorincz, K., Shnayder, V., Hauenstein, L., Dabiri, F., Jeng, J., et al. (2007). The advanced health and disaster aid network: A light-weight wireless medical system for triage. *Biomedical Circuits and Systems, IEEE Transactions on*, 1(3):203–216.

Google (2017). Google person finder web page. Available online: https://google.org/ (accessed on 15 February 2017).

Hespanha, J. P. (2004). An efficient matlab algorithm for graph partitioning. *Santa Barbara, CA, USA: University of California*.

Hoffman, K. L., Padberg, M., and Rinaldi, G. (2013). Traveling salesman problem. In *Encyclopedia of operations research and management science*, pages 1573–1578. Springer.

Inoue, S., Sonoda, A., Oka, K., and Fujisaki, S. (2006). Emergency healthcare support: Rfid-based massive injured people management. In *Proceedings of the fourth International Workshop on Ubiquitous Computing for Pervasive Healthcare Applications, Irvine, CA*.

Knox, R. W. (2015). Marcq saint-hilaire without tears. *The International Hydrographic Review*, 52(2).

Lee, J.-S., Su, Y.-W., and Shen, C.-C. (2007). A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi. In *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE*, pages 46–51. IEEE.

Malone-Lee, J. (2002). Identity-based signcryption. *IACR Cryptology ePrint Archive*, 2002:98.

Mudaliar, D. N. and Modi, N. K. (2013). Unraveling travelling salesman problem by genetic algorithm using m-crossover operator. In *Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013 International Conference on*, pages 127–130. IEEE.

Neuenschwander, M., Cohen, M. R., Vaida, A. J., Patchett, J. A., Kelly, J., and Trohimovich, B. (2003). Practical guide to bar coding for patient medication safety. *AMERICAN JOURNAL OF HEALTH SYSTEM PHARMACY*, 60(8):768–779.

of Medicine at NIH, N. L. (2017). People locator and reunite web page. Available online: https://lpf.nlm.nih.gov/ (accessed on 15 February 2017).

Rivero-Garcıa, A., Hernández-Goya, C., Santos-González, I., and Caballero-Gil, P. (2014). Fasttriaje: A mobile system for victim classification in emergency situations.

Santos-González, I., Rivero-García, A., Caballero-Gil, P., and Hernández-Goya, C. (2014). Alternative communication system for emergency situations. In *WEBIST (2)*, pages 397–402.

Sesia, S., Toufik, I., and Baker, M. (2009). *LTE: the UMTS long term evolution*. Wiley Online Library.

Smart, N. P. (2016). Hash functions, message authentication codes and key derivation functions. In *Cryptography Made Simple*, pages 271–294. Springer.

Want, R. (2011a). Near field communication. *IEEE Pervasive Computing*, (3):4–7.

Want, R. (2011b). Near field communication. *IEEE Pervasive Computing*, (3):4–7.

Zou, Z., Chen, Q., Uysal, I., and Zheng, L. (2014). Radio frequency identification enabled wireless sensing for intelligent food logistics. *Phil. Trans. R. Soc. A*, 372(2017):20130313.