Rivero-García *et al. J Wireless Com Network* (2021) 2021:202
https://doi.org/10.1186/s13638-021-02077-0

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A secure approach to monitoring emergency health resources

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

*Correspondence:
ariverog@ull.edu.es
Departamento de Ingeniería Informática y de Sistemas, Universidad de La Laguna, Tenerife, Spain

Abstract

This proposal presents an optimized, efficient and secure system designed to improve healthcare staff management in emergency situations through a complete tool to classify victims in a emergency situation according the severity of their condition, providing at the same time their location and the best route to reach them. The developed tool consists on a mobile application (assigned to medical and healthcare staff), a web service and Near Field Communication tags (assigned to victims). The mobile application supports secure communication among health staff and implements triage algorithms which result is stored in NFC tags. Apart from this, it helps to indicate which should be the next victim to be treated. The developed web service provides a global view of the emergency status and the current position of victims and staff. Data security is a key objective, overall in health applications; for this reason, tokens are used to protect the triage results before being stored in NFC tags, and the use of IDentity-Based Signcryption provides confidentiality and authentication to communications. Two different signcryption methods are used depending on the communication mode (peer-to-peer or broadcast mode).

Keywords: Emergency management, mHealth, Identity Based Signcryption (IBSC), Mobile application, Near Field Communication (NFC)

1 Introduction

Nowadays, most smartphones are used to support different daily tasks, due to their small size and high performance. Beside this, they are equipped with powerful communication technologies that can help in different scenarios. As far as the healthcare environment is concerned, there are studies, not very recent, that support the high penetration of mobile devices in the practice of medicine [1].

Based on this premise, this work presents a system, including mHealth solutions, that improves healthcare staff management in emergency situations thus impacting on a better and more efficient attention to victims. In order to achieve this goal, the system includes different aspects. One of the most significant is the implementation of algorithms for the classification of victims in emergency scenarios. These methods are traditionally referred to as triage. A triage may be defined as a simple, complete, objective and fast process to obtain an initial clinical assessment of casualties with the objective of evaluating their immediate survival capacities and prioritizing them according their

severity [2]. In order to classify victims, two steps are considered in all triage systems: a first triage or simple triage whose objective is obtaining a global assessment of the victim's survivability capabilities taking just some seconds, and a second triage, where health staff evaluates the state of each patient: injuries, bruises and wounds.

There is no standard triage system defined for catastrophes. The most used schemes in practice are START (Simple Triage and Rapid Treatment Algorithm) [3], JUMPSTART (a modification of START triage taking into account children) [4] and SIEVE [2]. For the second triage stage, MAT or SET [5] are the most common. The first triage is carried out in the emergency area, afterwards victims are moved to an Advanced Medical Position (AMP) where the second triage is performed. Finally, victims are evacuated to hospitals. The classification of victims generated in the first triage is based on colored tags, each color defines a different treatment priority: black, irrecoverable victims; red, victims requiring immediate care; yellow, victims requiring urgent care but can wait for treatment from half an hour to one hour; green, victims who are not seriously injured and can wait for treatment more than an hour. In traditional triage methods, tags are papers tags of 4 inch $\times$ 8 1/2 inch where health staff writes the classification and the result of the triage with a pen. Many are the reasons that makes this procedure not adequate for catastrophes [6]: environmental conditions may degrade information, it is difficult to keep up to date records of victim's condition, etc. The study presented in [7] supports that a mobile application has better liability and is more user-friendly than the traditional procedure for triage when naïve or less experienced staff carry it out.

These are some of the reasons why the use of Near Field Communication (NFC) tags to store triage result is proposed. Specifically, NFC stickers are used to store the information generated through an adaptation of a JSON Web Token (JWT) scheme (see Sect. 3). The priority of victims is reflected on the mobile devices of health staff through a map, allowing to trace the route to reach victims and geolocate them. Apart from this, health staff, in the affected area, can share information with their colleagues through an instant messaging service, supported by Wi-Fi Direct technology [8] and Bluetooth Low Energy (BLE) communications [9], using two modes: broadcast or peer-to-peer.

All this entire exchange of information is protected through an Identity Based Signcryption scheme (IBSC) [10].

This work is organized as follows. Section 2 provides an introduction to the state of the art on the area covered in this article. A global view of the proposal is described in Sect. 3. In Sect. 4, the system used to define the priority of victims is sketched out. The scheme defined to protect communications involving healthcare staff, an IBSC scheme, is proposed in Sect. 5. Section 6 contains a system analysis, and finally, conclusions and future works close the paper.

2 Related work

The integration of mobile devices and wireless communications into healthcare has generated new terms, such as mHealth. Penetration of these technologies in the field of health is currently very significant. One of the subjects that more attention has received in this environment is information security. In [11], a novel proposal to improve user authentication is proposed. Authors use facial image recognition and an algorithm to establish different access levels in m-health environments. The application described in

[12] is an example of solution for emergency response. A mobile application generates a map with recent emergency events; in the same map users may find the location of an automated defibrillator. CodeBlue system [13] is another example of mobile technologies in emergency situations. It is an U.S. Army system, centered on the use of wireless sensors in emergencies combining hardware and software platforms providing remote monitoring and tracking of patients and first responders [14]. These applications are not designed for large-scale emergency scenarios.

There are different proposals to help finding missing people after a large-scale disaster, such as Google Person Finder [15], People Locator and ReUnite [16] and Safety Check of Facebook. All these systems try to verify and share the status of people after a disaster. Specifically, Facebook's proposal uses notifications asking them to indicate if they are alright. Once answered, users can check if any of their friends are in the affected area and their status.

There are also some organizations working to provide solutions related to emergency situations. One of them is Sahana foundation [17] project, that aims to provide a set of modular, web-based disaster management applications. All the solutions are eHealth systems and include 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 with a centralized web-server, and thus, it cannot take advantages of mobile nodes. In the same line, a very useful tool is proposed in [18] consisting of software intended to manage data traffic efficiently in emergency situations taking place in smart cities.

An application designed to support pre-hospital emergency management is presented at [19]. As in our proposal, this application has a back-end service that enhances its functionalities, allowing to identify patients' condition, personal information and location. Anonymization is the only security service implemented for victim-related information. Given the characteristics of the information handled, anonymization alone is clearly insufficient. This system was tested by emergency medical staff.

In [20], a systematic and updated review of triage mobile applications is carried out. Authors state the interest of this solutions in recent years. Different approaches and technologies are present in the analyzed proposals. Among the criteria used in the comparison information security is not contemplated, and this is one of the main objectives in the system that we propose. The triage application included in our system met most of the recommendations drawn from this study since continuous care including the emergency scenario and geolocation service are provided.

In any emergency scenario, unambiguous identification of affected people must be a requirement. Traditional tag solutions are based on pre-written numbers that identifies patients. Barcodes are a possibility to consider as they facilitate the mechanical reading [21] and using them is a cheap and easy method to create identifications. They can be generated just using conventional devices such as printers, but in an emergency situation it is not a realistic approach.

Radio Frequency IDentification (RFID) is a very useful technology for victim identification, as it's explained in [22, 23]. Two types of tags are contemplated in this technology: 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. Specific hardware, for example RFID readers, is required when using this technology and there are many privacy and security concerns to overcame when using it in health application. In [24], a specific triage tag technology is proposed. These electronic triage tags use non-invasive biomedical sensors to continuously monitor the vital signs of patients and deliver pertinent information to their possible treatment. These are not tags suitable for emergency situations.

In [25], authors claims to solve victim identification problem through assigning an unique identifier (ID) to a device attached to the victim. This ID is also stored in an NFC-tag associated to the device. Nevertheless, the proposal does not include any protection mechanism for this identifier neither for the information related to the triage performed. Another work where an specific device is used for triage is [6]. It is focused on the design of the device although a mobile application is used for data acquisition, priority classification, data storage and data transfer to medical record server in hospitals. Again security mechanisms are not provided.

Reference [26] presents a routing protocol to guarantee communication within Wireless Body Area Networks defined to support an automated monitoring framework devoted to capture vital signs of casualties.

The use of NFC (Near Field Communication) [27] is one of the bases for automatic patient identification in the system proposed here. Specifically, NFC stickers are used. Some solutions based on these elements have been previously implemented, such as [28]. There a mobile system for victim classification in emergency situations was developed. The goal of this application is carrying out a first triage through a smartphone and storing its result in NFC tags. This system includes security schemes but it has a weakness, cloning NFC tags is possible.

Unlike technologies as Bluetooth, RFID [29] or Wi-Fi [30], NFC is not oriented to continuous data transmission. It's necessary a temporally contact between devices to allow a quick and instant information transfer. Although at first glance, proximity requirement may be seen as a limitation, it actually limits the types of attacksto deal with. Furthermore, since pairing between devices is not required its usability gets improved.

NFC devices may operate in two different modes: active and passive modes. In active mode, each device generates its own electromagnetic field (emulating the communication paradigm peer-to-peer). In passive mode, a device generates the electromagnetic field with its own power supply. In this way, it enables other device to start 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's the one used in this proposal.

Some of the key points and contributions of the system defined in this paper are summarized below:

- a tool to streamline the prioritization of victim assistance depending on their severity and location is provided. It includes the representation of the problem of allocating victims to MPAs and an algorithm to make such allocation cost-balanced.
- a secure communication channel for first-responders supported by Wi-Fi-Direct, and Bluetooth Low Energy technology is defined.

- a web application that allows the Visualization of the emergency status is included.
- a mobile application in charge of casualties triage, storing its protected output in NFC tags to store its result is supplied.
- all victim-related information is protected through specific mechanisms.
- unambiguous victim identification using NFC technology is achieved.
- dedicated devices are not required, so cost is reduced and deployment is simplified.

3 Global view

This paper presents a system based on [31] that may help to improve communication and management of first responders in real Mass Casualty Incident (MCI). Not all the emergencies are equal regarding resource management. This work is focused on MCI where multiple victims and the network infrastructure may be affected. The main objective is to generate a tool to save as much time as possible to treat victims in emergency situations.

It is assumed that in the incident area there is Wi-Fi Direct coverage and that the security procedures implemented in this wireless technology are robust.

Three basic areas may be distinguished at MCI (Fig. 1). The first zone is the rescue zone, where the basic triage is performed. In the treatment zone, the second triage to stabilize victims is performed jointly with the evacuation triage to define priority for evacuation of victims. The final zone is the hospital, where victims are treated if necessary.

The system provides a communication channel through a chat supported by Wi-Fi Direct on firs responders' mobile phones jointly with a map that helps them to locate the next victim to be treated and where the nearest point of medical attention is. Each triage location is represented in a map included in the web application. The order in which victims should be assisted is based on the severity of their injuries.

In this triage system, two stages are defined. The first one consists on evaluating victims at the affected area applying a first triage; we developed the JUMPSTART triage method to obtain victims classification using colored tags. This triage is generated by the first aid team including health personnel, fire-fighters or even rescue services.

The output of this step is a color for each patient, and it is stored on tags. In this case NFC tags, specifically NFC stickers, are used to save the triage result. The proposed

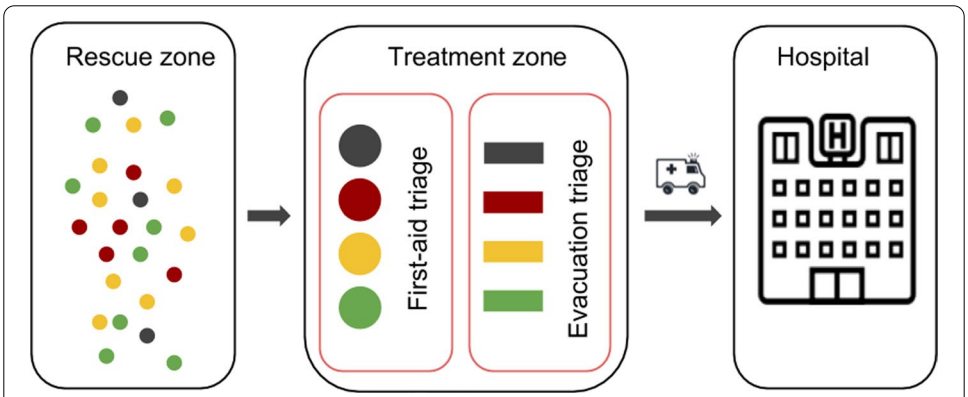


Fig. 1 Triage system schema

work uses NFC stickers but multiple kind of NFC tags can be used, it depends on the emergency and the victim state. The use of DESFire EV1 8K tag is recommended for this system.

In order to store the triage result in NFC stickers, an adaptation of JSON Web Token (JWT) is defined; The JSON header contains the algorithm used (HS256), and the payload is composed by the data related to the triage result, the identifier (ID) of each member of the healthcare workforce who has changed the content of the NFC sticker and a previous shared emergency code generated for each emergency situation, see Fig. 2. The JWT is stored on the NFC sticker.

JWTs allow platform-independent exchange of JSON-based information and, in this case, ensure the integrity of the information related to the triage result and identify who performed the triage.

In this case, the system stores 335 characters on the sticker and depends on the patient condition, the NFC tag used allows to store up to 7673 characters. Once the first triage is finished, the second stage may begin. In this step, victims' locations given by the first triage is the starting point.

In our system, the location of Advanced Medical Posts (AMPs) is decided taking into account the best route to evacuation (Fig. 3). Then, the assignation of patients to each AMPs is done automatically. Multiple variables are used for this task: triage color, AMPs workload and time required to transfer patients.

A star/tree subgraph is generated for each triage color. Vertices represent victim's and AMP's location. The nearest AMP is then assigned to each victim by defining an edge between them. The system generates as many trees as AMPs; the routes to reach them are the edges. Each edge has a cost associated defined as the distance between an AMP and a victim.

The Haversine Formula [32] has been chosen to calculate distance between two points. The notation required to define it is as follows: R the sphere radio, in our case the Earth's radio, γ_A, γ_B , respectively, stand for the latitudes of points A and B, $\Delta\lambda$ is the difference between both points longitudes. Considering $\text{sen}_{\gamma_{AB}} = \text{sen}(\gamma_A) \cdot \text{sen}(\gamma_B)$, $\cos_{\gamma_{AB}} = \cos(\gamma_A) \cdot \cos(\gamma_B)$, $d = d(A,B) = R * \arccos(\text{sen}_{\gamma_{AB}} + \cos_{\gamma_{AB}} * \cos(\Delta\lambda))$, the distance corresponds to the expression $\text{hvsin}(\frac{d}{R}) = \text{hvsin}(\gamma_A - \gamma_B) + \cos_{\gamma_{AB\Delta\lambda}}$ where hvsin is the haversine function: $\text{hvsin}(\theta) = \text{sen}^2(\frac{\theta}{2}) = \frac{1-\cos(\theta)}{2}$, and $\cos_{\gamma_{AB\Delta\lambda}} = \cos(\gamma_A) \cdot \cos(\gamma_B) \cdot \text{hvsin}(\Delta\lambda)$.

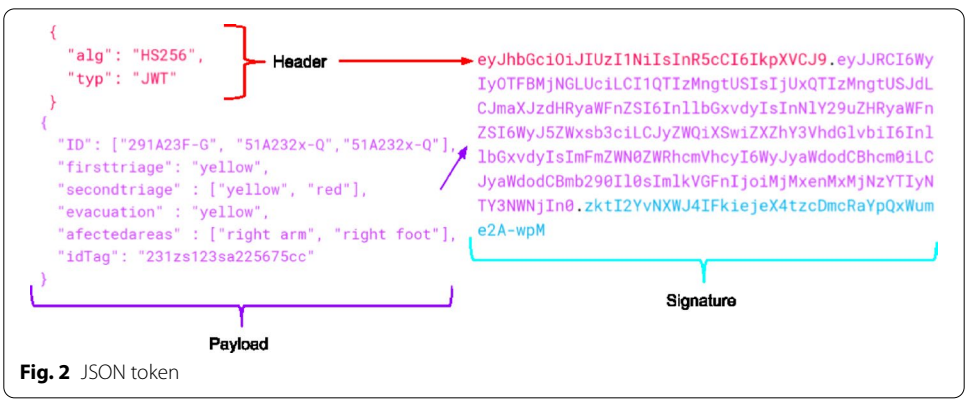
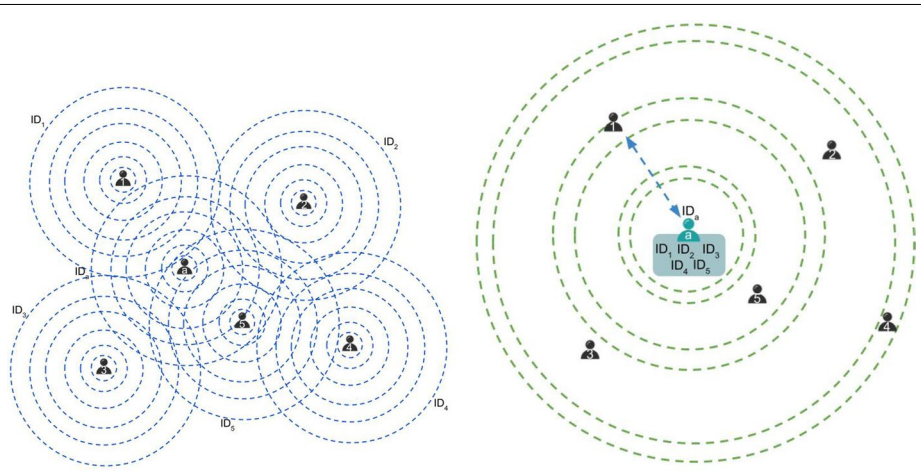


Fig. 2 JSON token

Fig. 3 Victims' and AMP's location



(a) Sharing credentials schema (b) Peer-to-peer and broadcast schema

Fig. 4 Communication modes

As it was previously stated, the system provides a secure communication channel through a chat supported by Wi-Fi Direct on first responders' mobile phones. It allows healthcare staff members to request help from a specific peer or from the closest ones. In order to identify the recipient of the chat messages, everybody share their own ID (it is a public information) through BLE by beacon mode, like in Fig. 4a. The fist time two healthcare staff members meet both exchange and store IDs. In this way, each peer will have a list of IDs belonging to nearby colleagues.

With this IDs list, health staff can share information using two communication modes: peer-to-peer mode or broadcast mode, as you can see in Fig. 4. Green lines are the broadcast communication and the blue ones, direct communication. In the broadcast mode, all health personnel in the affected area receive the notification and, simply by clicking on it, can initiate a chat.

When health staff arrives to a victim's location, the NFC sticker should be read with a mobile device, the person is assigned to an AMP, the point is marked as completed, and the status of next victim is checked.

4 Victim prioritization assistance tool

This section sketches the procedure used to define victims' priority. It is one of the innovations in this paper.

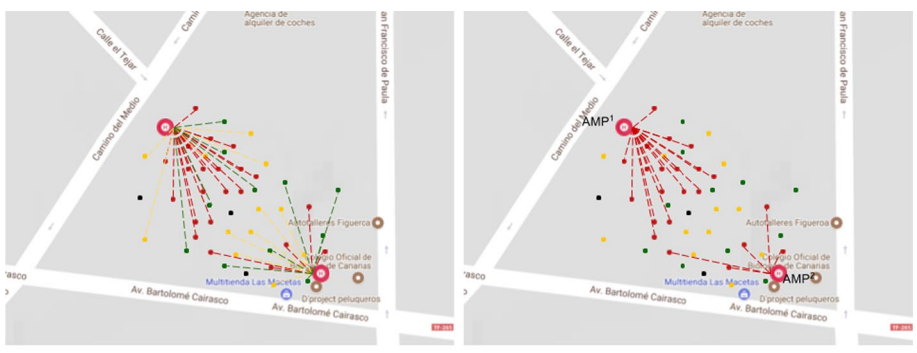
After the first triage, health staff transfer victims to the AMP to carry out the second triage. Position of different AMPs is previously defined. An undirected graph is generated from the points defined during the first triage.

Initially, our system assigns patients to each AMP depending on their relative position and distance. The main objective is to prioritize patients depending on the severity of their injuries. A first approach conveys the generation of different tree subraphs, as many trees as AMPs.

Every patient is originally assigned to an AMP according the cost associate to the edges. Patients with red triage are attended first, then patients with yellow triage and finally those with green triage Fig. 5a.

Black triage victims are assigned to the nearest AMP in order to be evacuated once the rest of the victims have been assisted.

In order to represent and analyze, this allocation problem an undirected graph $G = (V, K)$ is considered. V stands for the vertex set, and it comprises AMPs ("internal") nodes as well as victims nodes ("leaves"). The set of edges (K) is defined as the allocation of each victim to every single AMP. So $|V| = |K| + 1$. The edge cost function is denoted by $c : K \rightarrow [0, \infty)$. If S is a set of internal nodes, the final allocation will consist of as many trees as $|S|$. A *S-distribution* of K is a collection $P = \{K_1, K_2, \ldots, K_{|S|}\}$ of S disjoint subsets of K. Any *S-distribution* will define



(a) First approach (b) AMP saturation

Fig. 5 Victims' assignation based on nearest AMP

a solution to the allocation problem defined. A compromise solution will try to avoid *S-distributions* where the assignation of victims to AMPs will not be balanced (Fig. 5b).

An ad hoc rebalancing tree process is defined to deal with this issue. Once the first approach generates a feasible solution by considering the nearest AMP, the process of rebalancing tree is executed. Red points are evaluated, and each AMP calculates the cost of transfer all patients to them. This is the global cost for each AMP. The objective is reducing the cost by reassigning nodes. Then,the AMP with the highest global cost and the most expensive node is selected. The cost of migrating this victim to another AMP is calculated: the cheapest movement for the global cost of the corresponding AMP is selected. This approach is repeated until no more improvements in the movement of victims are detected. When the *S-distributions* built reach a cost balanced allocation of casualties, the system continues with the yellow output triages, then with the set of green nodes and finally with the black triages. A pseudocode of the algorithm developed is shown below (Algorithm 1).

```
Data: The first approach
Result: Balanced star trees
initialization();
while existCostImprovements AND existTriages do
    readCurrentCosts();
    getMoreExpensiveAMPCost();
    getMoreExpensiveNode();
    reassignmentCost = reassignment(moreExpensiveNode);
    if reassignmentCost < previousCost then
        updateInformation;
    else
        go back;
    end
end
```

Algorithm 1: Rebalancing triage algorithm

In case new victims are detected, the system automatically recalculates the trees using new nodes priority, and a new health staff's route is recalculated. The system assigns to each health staff member, depending on its location, the victim with the highest priority to be transferred to the AMP, where the second triage is developed.

A simulation has been carried out with the aim of validating this approach based on graphs. In the example shown in Fig. 5a, the solution is defined changing 4 nodes out of 22, resulting in 13 nodes at AMP^1 and 9 nodes at AMP^2 being the cost the same (Fig. 6). This is a basic example with red nodes to understand the algorithm, but several tests were generated with different number of nodes and random locations.

If a patient change his/her location and a health staff re-triages her/him, the system updates the information and the mobile application updates the NFC tag if necessary.

The incorporation of new health staff or new casualties does not cause any problems or additional cost. If more nodes are added to the graph, the priorities are updated paying attention to the new characteristics of the affected area. When a member of the health staff, in the affected zone, wants to access the triage result of a patient he/

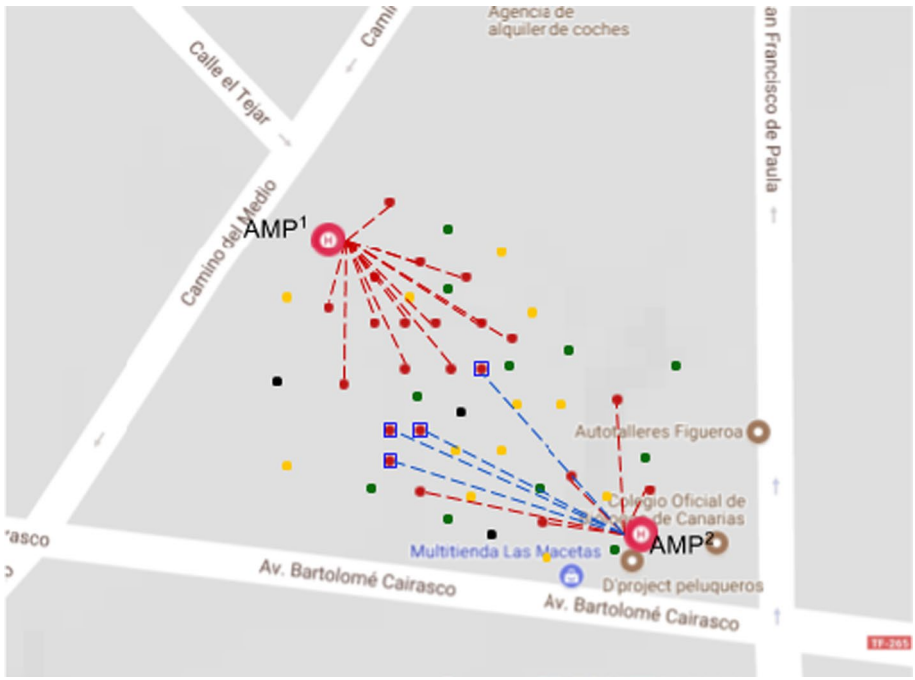


Fig. 6 Solution of rebalancing algorithm

she has to read the NFC sticker through the mobile application. Health staff can see all the nodes in their mobile phone, specifically the node she/he has to go next to treat a victim.

5 Health staff communication with signcryption scheme

One of the most important objectives of this work is the security of information related to healthcare in MCI. In this section, the description of one of the security mechanisms (IBSC schemes) used are included.

The implemented system supports two different communication modes: peer-to-peer mode and broadcast mode. In both communication modes, an ID-Based Signcryption scheme (IBSC) is used in order to achieve secure communications.

Health 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. This complex cryptosystem is a combination of an ID-Based Encryption (IBE) and an ID-Based Signature (IBS) providing private and authenticated delivery of information between two or more parties in an efficient way through the composition of an encryption scheme with a signature scheme [10]. This approach offers the advantage of simplifying key management since defining a public key infrastructure is not necessary. This kind of scheme was chosen due to its low computational complexity, efficiency, in terms of memory, and its usability.

The Private Key Generator (PKG), located at the central server, is a crucial part of the proposal because it is in charge of generating private keys for all the first responders.

In this implementation, the identifier (ID) assigned to each member of the health staff is the number associated to each registered medical practitioners or an specific

ID assigned when he/she is intended for such emergency. Next, we describe the mathematical basic tools used as well as their notation.

Considering two cycling groups $(G, +)$ and $(V, \cdot)$ of the same prime order q. P is a generator of G, and there is a bilinear map paring $\hat{e} : G \times G \rightarrow V$ 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: $H_1 : \{0,1\}^* \rightarrow G^*, H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*, H_3 : \mathbb{Z}_q^* \rightarrow \{0,1\}^n, H_4 : \{0,1\}^n \rightarrow \{0,1\}^{|m|}, H_5 : G \times G \times \{0,1\}^n \times Z_q^* \times Z_q^* \times \ldots \times Z_q^* \rightarrow Z_q^*$,
where the size of the message is defined by n. The signcryption scheme used is a combination between the ID-Based Signcryption Scheme proposed in [33] and ID-Based Signcryption Scheme for Multiple Receivers. Here, $x \xleftarrow{r} S$ 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 first two steps are common to both versions of the protocol since they are responsible for the configuration tasks and the generation of the secret information associated with each staff member, respectively.

Next, the description of all these steps is included:

- *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 $\hat{e} : G \times G \rightarrow V$ 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* In this step, the secret key for each member of the health 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 users is performed using the stream cipher SNOW3G [34] under the session key obtained through an Elliptic Curve Diffie–Hellman (ECDH) [35].

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

- *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 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).

$$
\begin{aligned}
&Q_{ID_b} \leftarrow H_1(ID_b)\\
&x \xleftarrow{r} \mathbb{Z}_q^*\\
&T \leftarrow x \cdot P\\
&r \leftarrow H_2(T||m)\\
&W \leftarrow x \cdot mpk\\
&U \leftarrow r \cdot S_{ID_a} + W\\
&y \leftarrow \hat{e}(W, Q_{ID_b})\\
&k \leftarrow H_3(y)\\
&c \leftarrow k \oplus m\\
&\sigma \leftarrow (c, T, U)
\end{aligned}
$$

- *SINGLE UNSIGNCRYPTION* 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}.

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

Verification:

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

- *MULTIPLE RECEIVER SIGNCRYPTION* If there are n receivers, the system has to deal with several identifiers $ID_1, ID_2, \ldots, ID_n$. The sender identifier is ID_a. All the broadcasted messages $m \in \{0,1\}^n$ will be encrypted and signed. The receivers' public keys are generated taking into account all the identificatiers $ID_1, ID_2, \ldots, ID_n$ giving as result σ (a t-uple of three components:$c, T, U, Y, W, a_0, \ldots a_n - 1$)

$$Q_{ID_a} \leftarrow H_1(ID_a)$$
$$x \overset{r}{\leftarrow} \mathbb{Z}_q^*$$
$$T \leftarrow x \cdot P$$
$$Y \leftarrow x \cdot Q_{ID_a}$$
$$\alpha \overset{r}{\leftarrow} \mathbb{Z}_q^*$$
$$U \leftarrow \alpha \cdot Y$$
$$W \leftarrow x \cdot mpk$$
$$p \overset{r}{\leftarrow} \mathbb{Z}_q^*$$
$$v_i \leftarrow H_2(\hat{e}(Q_i, W))$$
$$Q_i \leftarrow H_1(ID_i)$$
$$f(x) = \prod_{i=0}^{n} (x - v_i) + p(mod q) =$$
$$= a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$
$$\beta \overset{r}{\leftarrow} \mathbb{Z}_q^*$$
$$c \leftarrow \beta \oplus H_3(p)$$
$$K \leftarrow H_4(\beta)$$
$$Z \leftarrow Snow3G_K(m)$$
$$h \leftarrow H_5(c, T, U, Z, a_0, a_1, \ldots, a_{n-1})$$
$$W \leftarrow (\alpha + h)r \cdot S_{ID_a}$$
$$\sigma \leftarrow (c, T, U, Y, Z, a_0, \ldots, a_{n-1})$$

- *MULTIPLE RECEIVER UNSIGNCRYPTION* If everything is right, the message $m \in \{0,1\}^n$ is returned. Two verifications are realized, public verification to check that the ciphertext is valid ($\hat{e}(W, P) == \hat{e}(U + hY, mpk)$). Otherwise, the ciphertext has been damaged or it is invalid and $\perp$ is returned. The second verification ($\hat{e}(W, Q_i) == \hat{e}(X + hY, mpk)$), 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.

  $$h \leftarrow H_5(c, T, U, Z, a_0, a_1, \ldots, a_{n-1})$$

  Verification:

  $$\hat{e}(W, P) == \hat{e}(U + hY, mpk)$$

  Verification:

  $$\hat{e}(W, Q_i) == \hat{e}(X + hY, mpk)$$
  $$y \leftarrow H_2(\hat{e}(S_{ID_b}, T))$$
  $$v_i \leftarrow H_2(y)$$
  $$p \leftarrow f(v_i)$$
  $$\beta \leftarrow c \oplus H_3(p)$$
  $$K \leftarrow H_4(\beta)$$
  $$m \leftarrow Snow3G_K(Z)$$

6 Results and discussion

In this section, an analysis of the proposed communication architecture, its communications and its security is provided.

A flowchart illustrating system communication is shown in Fig. 7.

First of all, health staff workers need to be previously registered and authenticated by the manager at the server. The manager have a global view with all the events through the web application and will be responsible for the emergency management. He is also registered on the system and has the possibility of modifying the staff information if necessary.

The key generator corresponds to a service running in the server as second process and generating keys to protect communications.

Once the manager assigns a worker to a emergency (1) he/she obtains the information related to the event and his/her intervention on the affected area (2). If the first responder finds a new victim, he/she makes a first triage and stores the output on a new NFC tag (3). In other case, if the worker finds a victim who is already registered he/she reads the NFC tag, analyzes the information and updates it if necessary (4).

Note that first reponders' routes depend on the triage they carry out. When a new patient is found, extra information is not needed. Otherwise, next victim to attend is decided depending on the priority defined by the previous triages performed on him/her.

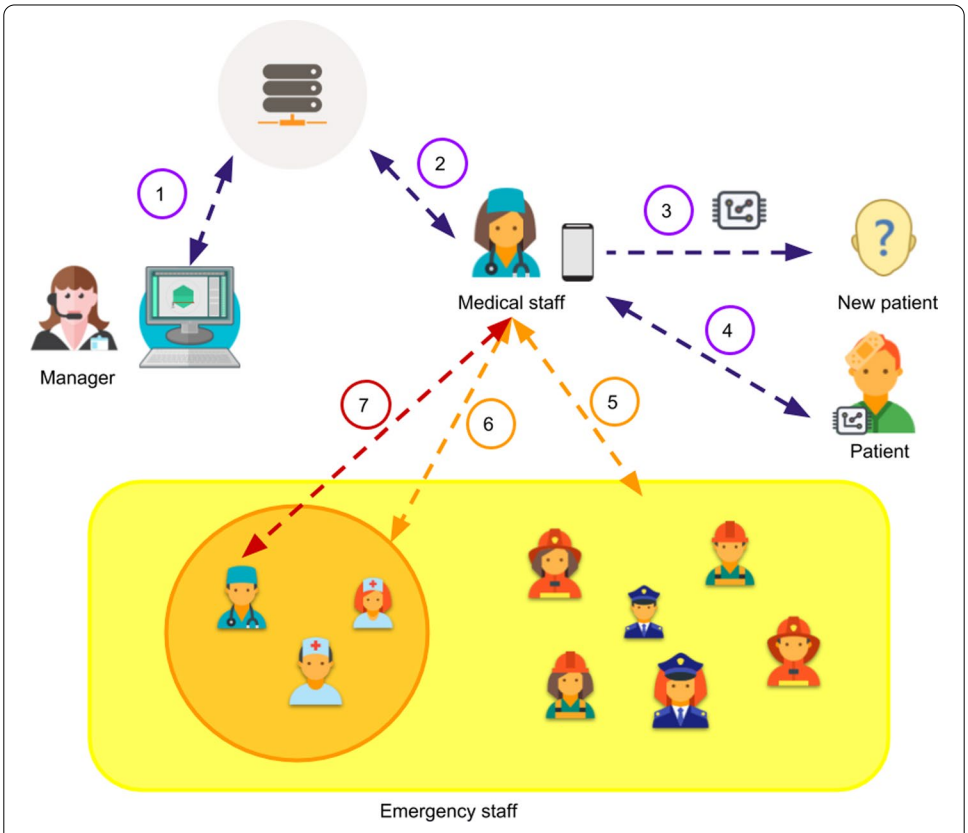


Fig. 7 Communication flow

Finally, the worker can send information to a group (based on an specific role), for example to doctors (6) (7), or a direct message to another peer (7).

6.1 Simulation and efficiency analysis

A prototype of the system has been developed, with a web application (see Fig. 8a) and a mobile application (see Fig. 8b).

The implementation comprises:

- a web application developed with JavaScript in the backend (with Nodejs) and Vuejs in the frontend,
- a mobile application implemented in Android with Kotlin and the 5.5 SDK version

Regarding the hardware, a laptop with Windows x64 and 16 GB RAM was used for the web application and a Pixel 2 with Android to run the mobile application.

A simulation tool has been developed based on JavaScript and the Google maps API in order to validate the approach proposed to assign resources. It also allows to represent and monitoring the emergency situation.

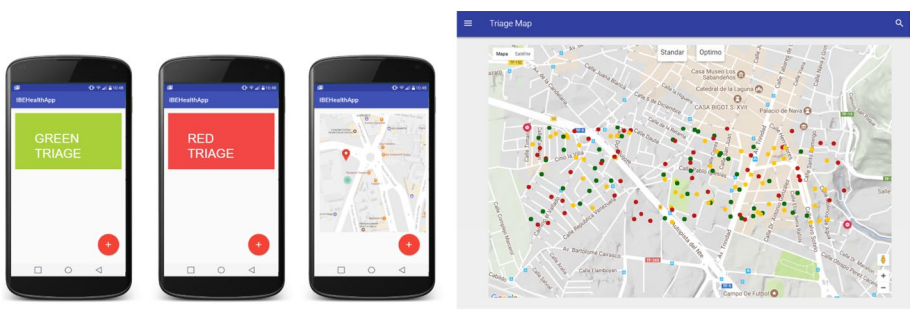
Some random points of different colors representing people affected by the emergency have been generated and located on the map. Colors are the result of the first triage (red, yellow, green and black). In Fig. 9, the costs of the naïve approach (allocation to the nearest AMP) and the one defined in this paper are compared. The blue part is the cost of traditional method, and the black part is the cost of the proposed system. The improvement of black zone over blue one is observable. In this case, the evaluation is supported by the output of 100 iterations with 1000 victims.

In Fig. 10, improvements for 100 iterations with different victims amount are represented. In all the cases, there are improvements. Note that all the locations in the simulations where randomly generated, and the output of this figure is the mean of all solutions of iterations.

The code of the testing tool is available in a Github repository [36].

6.2 Security analysis

In the system developed, standard signcryption protocols are used in order to guaranteeing confidentiality and authenticity of data by combining signature and encryption



(a) Mobile application (b) Web application

Fig. 8 Developed prototype

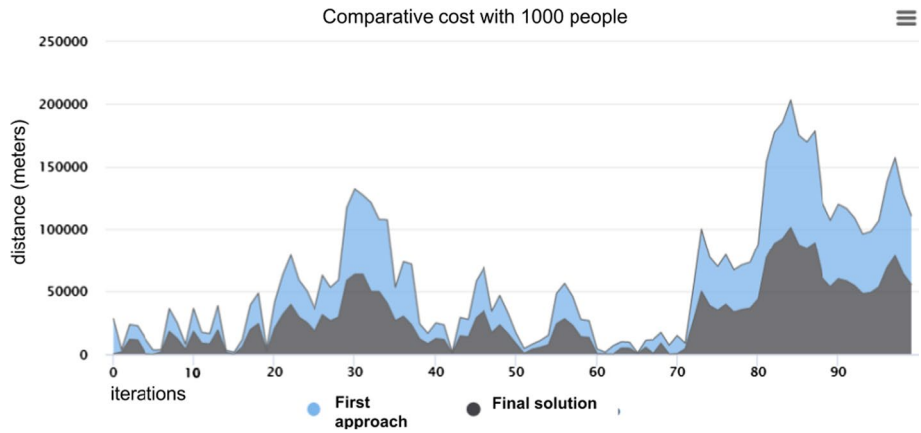


Fig. 9 Costs of allocating victims

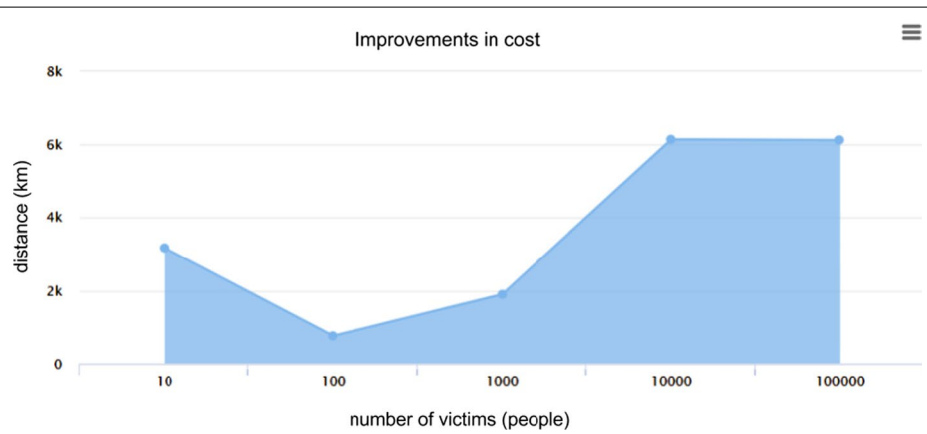


Fig. 10 Improvements

while communication overhead and computational costs are reduced. Details on the formal security analysis of signcryption protocols may be fount at [37].

During Unsigncryption, user B computes $y \leftarrow H_2(\hat{e}(S_{ID_b}, T))$ to retrieve the ephemeral session key k used to encrypt the message m. Only the intended recipient in possession of the private key can retrieve this value. Otherwise, it will be necessary to invert the hash function H_2 and solving instances of the Elliptic Curve Diffie–Hellman problem.

For sender identification verification, the signature must be verified using both the public key Q_{ID_a} of the sender and the master public key (mpk) by user B. Obtaining user keys while they are distributed by the PKG is not viable since that are sent ciphered with SNOW3G.

In the multiple receiver signcryption, the message m is encrypted by the sender using Snow3G with an ephemeral key K derived from randomly selected integers. This k may be calculated only by the intended recipients since it is calculated as the output of a hash function over a secret information. Again, signature verification requires the public keys of users and master.

Forward secrecy is also achieved thanks to the use of ephemeral ciphering keys. Although an adversary managed to know sender's secret keys, deciphering previous messages will not be possible since ciphering keys are derived from random information that change for every message sent.

The proposed scheme provides protection against different attacks. Attacks related to multiple requests to the server, Denial of Service (DoS) attack, are restricted because only requests associated with a number of legitimate members of the health staff will take effect.

Once the corresponding private key is assigned, no more requests of this kind will be attended. Thus, the typically "Man in the Middle" (MiTM) attack which conveys a successful authentication to the server with an identifier of legitimate members of the health 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 [38]. It should be clarified that resistance to certain types of attacks such as DOS and MiTM is not a feature of the algorithm but of the specific application domain. When using it in a different domain, its invulnerability to the same attacks can not be guaranteed.

7 Conclusions and future work

Finally, some conclusions and future works close the paper. A prototype, in Android and Nodejs with NFC tags, to improve logistics and attention of casualties in extreme situations has been developed. The main contribution of the paper is the development of a secure tool for the management of victims in emergencies situation. The tool consists on a mobile application, NFC tags and a web application. With the mobile application health staff know at any time which is the next victim to be treated. Our system automatically generates the assignment of patients to each AMP based on their position.

An emergency support channel to contact peers through a chat when health staff require additional support is included as well. Data security is a key objective, so for this reason ID-Based Signcryption is used for protecting communications. Several simulations where realized with different amount of casualties in order to validate the tool proposed. Summing up, contributions of this system are manyfold. The system allows the management of victims and emergency resources as well as, the classification and identification of patients though a triage application. A dynamic algorithmic solution to the problem of victim allocation to AMPs is also proposed. Note that efficiency has been tested through some experiments.

Special attention has been paid to the security of information related to victims and responders by developing specific protocols.

As future work, more functionalities can be added to the web platform, such as, more statistics about the state of the emergency scenario in order to define a heat map to identify the most affected area.

Direct communication (peer-to-peer) between the manager and a staff member participating in the event is a work in progress task.

A real time test with the emergency response staff will be really interesting to analyze the performance of the tool and detecting its weaknesses.

The authors declare that there is no conflict of interest regarding the publication of this paper, and the simulations generated with the data that support the findings of this study are available in a Github repository [36].

Acknowledgements
Research supported by TESIS2015010102, TESIS2015010106, RTC-2014-1648-8, TEC2014-54110-R, MTM-2015-69138-REDT, DIG02-INSITU and RTI2018-097263-B-I00: ACTIS.

Authors' contributions
All authors read and approved the final manuscript.

Received: 9 August 2019 Accepted: 9 December 2021
Published online: 20 December 2021

References

1. N. Koehler, O. Vujovic, C. Mcmenamin, Healthcare professionals' use of mobile phones and the internet in clinical practice. J. Mob. Technol. Med. (2013). https://doi.org/10.7309/jmtm.2.1.2
2. A. Garner, A. Lee, K. Harrison, C.H. Schultz, Comparative analysis of multiple-casualty incident triage algorithms. Ann. Emerg. Med. **38**(5), 541–548 (2001)
3. C.A. Kahn, C.H. Schultz, K.T. Miller, C.L. Anderson, Does start triage work? an outcomes assessment after a disaster. Ann. Emerg. Med. **54**(3), 424–430 (2009)
4. L.E. Romig, Pediatric triage. A system to JumpSTART your triage of young patients at MCIs. JEMS J. Eemerg. Med. Serv. **27**(7), 52–8 (2002)
5. J Gómez. Jiménez, F Boneu Olaya, O Becerra Cremidis, E Albert Cortés, J Ferrando Garrigós, M Medina Prats, Validación clínica de la nueva versión del programa de ayuda al triaje (web_e-pat v3) del modelo andorrano de triaje (mat) y sistema español de triaje (set). fiabilidad, utilidad y validez en la población pediátrica y adulta. Emergencias **18**(4), 207–214 (2006)
6. M. Niswar, A.S. Wijaya, M. Ridwan, Adnan, A.A. Ilham, R.S. Sadjad, A. Vogel, The design of wearable medical device for triaging disaster casualties in developing countries, in *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)* (2015), pp. 207–212. https://doi.org/10.1109/ICDIPC.2015.7323030
7. S. Savatmongkorngul, C. Yuksen, C. Suwattanasilp, K. Sawanyawisuth, Y. Sittichanbuncha, Is a mobile emergency severity index (ESI) triage better than the paper ESI? Intern. Emerg. Med. **12**(8), 1273–1277 (2017). https://doi.org/10.1007/s11739-016-1572-x
8. M. Condoluci, L. Militano, A. Orsino, J. Alonso-Zarate, G. Araniti, Lte-direct vs. wifi-direct for machine-type communications over lte-a systems, in *2015 IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (IEEE, 2015), pp. 2298–2302
9. E. Mackensen, M. Lai, T.M. Wendt, Bluetooth low energy (BLE) based wireless sensors, in *Sensors, 2012 IEEE* (IEEE, 2012), pp. 1–4
10. X. Boyen, *Identity-Based Signcryption* (Springer, Berlin, 2010)
11. F.D. Guillén-Gámez, I. García-Magariño, J.B. Agapito, R. Lacuesta, J. Lloret, A proposal to improve the authentication process in m-health environments. IEEE Access **5**, 22530–22544 (2017). https://doi.org/10.1109/ACCESS.2017.2752176
12. Pulsepoint respond app (2013), https://www.pulsepoint.org/. Accessed Nov 2021
13. K. Lorincz, D.J. Malan, T.R. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, S. Moulton, Sensor networks for emergency response: challenges and opportunities. IEEE Pervasive Comput. **3**(4), 16–23 (2004)
14. C. Blue, Code blue platform (2017), http://codeblue.com/applications/, http://codeblue.com/applications/. Accessed May 2018
15. Google, Google person finder web page (2017), https://google.org/, https://google.org/personfinder/global/home.html. Accessed May 2018
16. N. L. of Medicine at NIH, People locator and reunite source code (2017), https://github.com/lhncbc, https://github.com/lhncbc/Reunite-Android. Accessed Nov 2018
17. S. Foundation, Open source disaster management software (2017), https://sahanafoundation.org/, https://sahanafoundation.org/products/. Accessed May 2018
18. A. Rego, L. García, S. Sendra, J. Lloret, Software defined network-based control system for an efficient traffic management for emergency situations in smart cities. Future Gener. Comput. Syst. **88**, 243–253 (2018). https://doi.org/10.1016/j.future.2018.05.054
19. A. Nimmolrat, K. Sutham, O. Thinnukool, Patient triage system for supporting the operation of dispatch centres and rescue teams. BMC Med. Inform. Decis. Mak. **21**(1), 68–68 (2021). https://doi.org/10.1186/s12911-021-01440-x
20. I.H. Montano, I. de la Torre Díez, R. López-Izquierdo, M.A.C. Villamor, F. Martín-Rodríguez, Mobile triage applications: a systematic review in literature and play store. J. Med. Syst. **45**(9), 86 (2021). https://doi.org/10.1007/s10916-021-01763-2
21. M. Neuenschwander, M.R. Cohen, A.J. Vaida, J.A. Patchett, J. Kelly, B. Trohimovich, Practical guide to bar coding for patient medication safety. Am. J. Health Syst. Pharm. **60**(8), 768–779 (2003)
22. B.P. Rosenbaum, Radio Frequency Identification (RFID) in health care: privacy and security concerns limiting adoption. J. Med. Syst. (2014). https://doi.org/10.1007/s10916-014-0019-z
23. Baracoda, Idblue—an efficient way to add RFID reader/encoder to bluetooth PDA and mobile phones (2017), http://www.baracoda.com, http://www.baracoda.com/baracoda/products/p21.html. Accessed May 2018

24. T. Gao, T. Massey, L. Selavo, D. Crawford, B.-R. Chen, K. Lorincz, V. Shnayder, L. Hauenstein, F. Dabiri, J. Jeng et al., The advanced health and disaster aid network: a light-weight wireless medical system for triage. IEEE Trans. Biomed. Circuits Syst. **1**(3), 203–216 (2007)
25. A. Rigos, E. Sdongos, F. Misihroni, A. Stamou, P. Kuqo, E. Latsa, A. Amditis, A novel triage system using bluetooth devices in support of incident management, in *2019 13th International Conference on Sensing Technology (ICST)* (2019), pp. 1–5. https://doi.org/10.1109/ICST46873.2019.9047744
26. D. Olivia, A. Nayak, M. Balachandra, Data-centric load and QoS-aware body-to-body network routing protocol for mass casualty incident. IEEE Access **9**, 70683–70699 (2021). https://doi.org/10.1109/ACCESS.2021.3077472
27. R. Want, Near field communication. IEEE Pervasive Comput. **10**(3), 4–7 (2011). https://doi.org/10.1109/MPRV.2011.55
28. A. Rivero-Garcıa, C. Hernández-Goya, I. Santos-González, P. Caballero-Gil, Fasttriaje: a mobile system for victim classification in emergency situations, in *Proceedings of the 10th International Conference on Web Information Systems and Technologies - Volume 1: WEBIST* (2014), pp. 238–242
29. Z. Zou, Q. Chen, I. Uysal, L. Zheng, Radio frequency identification enabled wireless sensing for intelligent food logistics. Philos. Trans. R. Soc. A **372**(2017), 20130313 (2014)
30. J.-S. Lee, Y.-W. Su, C.-C. Shen, A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and WI-FI, in *33rd Annual Conference of the IEEE Industrial Electronics Society, 2007. IECON 2007* (IEEE, 2007), pp. 46–51
31. A. Rivero-García, I. Santos-González, C. Hernández-Goya, P. Caballero-Gil, IBSC system for victims management in emergency scenarios, in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, IoTBDS 2017*, Porto, Portugal, April 24-26 (2017), pp. 276–283. https://doi.org/10.5220/0006298702760283
32. R. W. Knox, Marcq saint-hilaire without tears. Int. Hydrograph. Rev. **52**(2), 169–172 (2015)
33. J. Malone-Lee, Identity-based signcryption, IACR Cryptology ePrint Archive 2002 (2002) 98
34. I. Santos-González, A. Rivero-García, P. Caballero-Gil, C. Hernández-Goya, Alternative communication system for emergency situations, in *WEBIST (2)* (2014), pp. 397–402
35. J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, E. Wustrow, Elliptic curve cryptography in practice, in *International Conference on Financial Cryptography and Data Security* (Springer, 2014), pp. 157–175
36. A. Rivero, Simulations of the data (2018), https://github.com/alelit4/TriageMap, https://github.com/alelit4/TriageMap. Accessed June 2018
37. J. Baek, R. Steinfeld, Y. Zheng, Formal proofs for the security of signcryption. J. Cryptol. **20**(2), 203–235 (2007). https://doi.org/10.1007/s00145-007-0211-0
38. M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, K. Sakurai, Authentication in mobile cloud computing: a survey. J. Netw. Comput. Appl. **61**, 59–80 (2016)

Publisher's Note