m-Carer: Privacy-Aware Monitoring for People with Mild Cognitive Impairment and Dementia

Agusti Solanas, Member, IEEE, Antoni Martínez-Balleste, Member, IEEE, Pablo A. Perez-Martinez, Albert Fernandez de la Pena, and Javier Ramos

Presented By: Kevin Di Benedetto
SUNY Binghamton University
September 19th, 2014
Overview

- Brief Description of MCI and Dementia [Background]
- Formal Statement of Problem
- Current Best Practice and Limitation
- Privacy-Aware Approach [Novelty]
- Rationale, Concept, and Desiderata
- Running Example
- Structure, Actors, and Roles
- M-Carer Operation and Alarm States
- Registration of Patients and Unofficial Users
Overview (Contd.)

- State of No Alarm (NA)
- State of Non-Critical Alarm (NCA)
- State of Critical Alarm (CA)
- Obtaining Information
- Conclusions and Future Work
- Questions
Brief Description of MCI and Dementia

[Background]

- Mild cognitive impairment (MCI) is an intermediate stage between the expected cognitive decline of normal aging and the more serious decline of dementia. It can involve problems with memory, language, thinking and judgment that are greater than normal age-related changes.

- Dementia is a chronic or persistent disorder of the mental processes caused by brain disease or injury and marked by memory disorders, personality changes, and impaired reasoning.

- Said illnesses can drastically effect how one lives their life.

- Mild Cognitive Impairments are a precursor to dementia.
Formal Statement of Problem

- When patients with cognitive impairments wander away and get lost, they may have serious or even fatal accidents – they can become spatially and temporally disoriented.
- Over 40% of patients with dementia get lost outside their homes – this is a significant portion of people with dementia!
- To avert said situation, carers supervise patients and keep them safe. This often requires to lock doors or preventing the patient from leaving in other ways such as constant surveillance or putting them on drugs.
- These methods limit the sense of freedom of patients and could have negative effects on their well-being.
- Rapidly determining the location of a lost patient is paramount to reduce the risk of suffering serious injuries.
Current Best Practice and Limitation

- The use of mobile phones equipped with GPS to *continuously* track patients was proposed.
- The main problem encountered by researchers was user compliance! The proposed system instills the “Big Brother” effect in patients.
- Such continuous control might be seen by most people as a privacy invasion, and it may discourage patients from using these solutions – this can be a serious safety concern.
- Patients, and their caretaker(s), desire to feel comfortable with solutions to this issue – they are patients not prisoners!
Privacy-Aware Approach [Novelty]

- Proposed m-Carer as a smart mobile device able to *privately monitor* the movements of patients.
- A complete architecture aimed at fulfilling the needs of patients, relatives, and health care services was proposed.
- If no special events happen, the system must prevent users from locating patients, thus, preserving their fundamental right to privacy. [More on special events later.]
- The m-Carer solution is not aimed at replacing human carers, but to provide them with a powerful tool able to simplify their job, improve their efficiency, reduce costs, and keep the fundamental rights of their patients fully guaranteed.
Privacy-Aware Approach [Formal Definition]

“A mobile carer m-Carer is a mobile device and an infrastructure that provides patients and users with health-care monitoring services in a private, reliable, and personalized way.”
Rationale, Concept, and Desiderata

- An m-Carer is a mobile device and an infrastructure that provides patients/users with health-care monitoring services in a private, reliable, and personalized way.

- The act of supervision should be private to avert any hindrance from the patient - avoiding the “Big Brother” effect is paramount to guarantee the acceptance of patients with a high degree of autonomy.

- If alarm conditions are not met the location of patients should be kept secret.

- The m-Carer system must be able to detect situations in which the safety of the patient is in danger.
Rationale, Concept, and Desiderata [Contd.]

- Dangerous situations for the patient could range from being in an area with a cliff to wandering a significant distance from a place that is deemed to be safe, like their home.

- The patient could have been physically injured and would need immediate assistance.

- The patient might be in an unusual place, with respect to the patients regular spacial locality, and would also need immediate assistance to prevent possible catastrophic events from occurring.
Rationale, Concept, and Desiderata [Contd.]

- The m-Carer system should not need any collaboration from the patient.
- The m-Carer must be simple and easy to use, even to patients that are not familiar with information and communication technologies.
- The embodiment of the m-Carer should be simple and usual – it should not seem as something strange or intrusive.
- These outlined requirements, in aggregate, should make the system user friendly and patients should have no reason to reject it.
Running Example

- Throughout this presentation, an example will be referred to so as to show the specific functionality of the m-Carer proposal.
- It is desired to show that the architecture has a clear and direct application to real life situations.
- The patient in question is named John Oldsmith and he suffers from Alzheimer's disease, which is coincidentally the most common form of dementia. He has decided to take up residence in a renowned old people's home – The Golden Yard.
- John has a daughter, Ellie, who takes care of Mr. Oldsmith.
Running Example [Contd.]

- Mrs. Andrews, the head of The Golden Yard carers asks John to carry a GPS-enabled necklace that allows her to know the location of Mr. Oldsmith at any moment.
- This was asked of the patient on a “just in case” manner.
- Despite the way the GPS-enabled necklace was presented to Mr. Oldsmith, Mrs. Andrews says that Mr. Oldsmith feels that his privacy is being invaded, and that he has to choose between his promenades (his daily walks) and his privacy.
- More on this example later...
Running Example [Illustrated]
Structure, Actors, and Roles

- The m-Carer (an essential actor of the system) is an application that runs on a smart phone able to locate itself by means of GPS, WiFi, or fixed antennas trilateration.
- The application is able to encrypt information and to send it to a server or a set of servers that store it.
- The m-Carer uses the telecommunications infrastructure that already exists and does not require any additional device (apart from the smart-phone).
- The system considers a number of human actors, namely patients, official users and unofficial users.
Structure, Actors, and Roles [Contd.]

- **Patients** - people that are able to move autonomously (e.g. have a walk, go shopping, etc.) that due to their cognitive impairments might get lost and require assistance.

- To avert the “Big Brother” effect, the m-Carer encrypts their information.

- Patients are equipped with a GPS-enabled smart-phone connected to the Internet. We refer to this device as **Patient's Device** in which the m-Carer application runs.

- In the running example, John Oldsmith is the **patient**. Mr. Oldsmith owns a simple smart-phone, equipped with GPS and a 3G data connection - he has installed the m-Carer application in his smart-phone and he has signed in the system.
Structure, Actors, and Roles [Contd.]

- **Users** - people ethically or legally responsible for the supervision of *patients* (e.g. human carers, relatives, friends, etc).

- While the privacy of the patients is one of the main priorities for the system, for the sake of safety, users are allowed to know the location of patients in some specific situations.

- Similarly to *patients*, *users* are equipped with a smart-phone running a User application - users can interact with the system and receive notifications from their application.

- **Official users** are people that are legally responsible for the well-being and safety of patients such as social workers, doctors, nurses, or public human carers. In the running example, Mrs. Andrews is the *official user* for all the *patients* living in The Golden Yard.
Structure, Actors, and Roles [Contd.]

- **Unofficial users** - people related to the *patient*, namely relatives, friends and private human carers – they might be in charge of *patients* and would need to know where they are, especially if they tend to get lost.

- In the running example, Ellie (Mr. Oldsmith's daughter), is the *unofficial user* responsible for the safety of Mr. Oldsmith, who is the *patient*.

- **Emergency Services** - actors that ensure public safety by addressing emergencies (e.g. firemen and rescue services, medical emergencies, etc.) - in normal conditions, these *emergency services* do not play an active role in the system.

- Help is required when an emergency situation arises. The m-Carer is responsible for informing *emergency services* and for asking for their help when a critical emergency is detected.
Structure, Actors, and Roles [Contd.]

- **Servers of the System** - The system comprises a set of servers that support its operation and provide additional functions - mobile applications interact with these servers by using the already present infrastructure of the telephony company and the Internet service provider.

- **Servers of Preferences** - allows the registration of patients and users into the system - they are responsible for the generation of the cryptographic keys to be used by the m-Carer and the User applications. They allow users and patients to tune several parameters of the system that controls its behavior. By doing so, users and patients can customize the service provided by the m-Carer and make it to better suit their needs.
Structure, Actors, and Roles [Contd.]

- **Location Servers** - receive encrypted location information from the m-Carer of the patients and store it - these servers could receive other data (e.g. heartbeat rate, body temperature, etc.). All this information is encrypted and the server does not have access to the cryptographic keys to decrypt it. Location servers can be understood as log servers that store information of the whole system.
Structure, Actors, and Roles [Illustrated]
Structure, Actors, and Roles [Illustrated]
M-Carer Operation and Alarm States

- There are two main types of tasks, administrative tasks and monitoring tasks.
- Administrative tasks are mainly related to the registration of users and patients into the system, the management of cryptographic keys, and the disclosure of information that requires the intervention of multiple parties.
- Monitoring tasks are essentially focused on the analysis of location information with the aim to detect situations that could endanger the safety of the patients.
- In general, administrative tasks involve several actors (patients, users, servers, etc.) whilst monitoring tasks are essentially performed by the m-Carer running on the patients' devices.
Registration of Patients and Unofficial Users

- Adding a patient to the system can only be done by an official user.
- They access the **Server of Preferences** to register the new patient, as well as one of more unofficial users related to the patient.
- The server generates the cryptographic keys required by the system's protocol.
- Public and private key pairs are generated for the unofficial users: \{\text{Pk}_{\text{uu}}, \text{Sk}_{\text{uu}}\}.
- Public and private keys are created for the m-Carer running on the **patient's device**: \{\text{Pk}_{\text{pd}}, \text{Sk}_{\text{pd}}\}. 
Registration of Patients and Unofficial Users [Contd.]

- A random encryption key \( \{K_{pd}\} \) is generated for the patient's device – it's stored in the server of preferences and known to the patient's relatives and caretakers.

- It is assumed that official users already have a public and private key pair \( \{Pk_{ou}, Sk_{ou}\} \).

- Keys \( \{Sk_{pd}, Pk_{uu}, Pk_{ou}, K_{pd}\} \) and the m-Carer applications are installed into the patient's device.

- The key \( \{K_{pd}\} \) is sent to the location server and it is associated with the patient's device.

- Keys \( \{SK_{uu}\} \) and \( \{SK_{ou}\} \) are stored in the server of preferences, with password protection that is known only by the owners of the keys.
Registration of Patients and Unofficial Users [Illustrated]
State of No Alarm (NA)

- If the m-Carer running in the patient's device does not detect any of the alarm conditions defined, it periodically sends encrypted data to the Location server.

- The data is encrypted with the public key of the Unofficial user, and the result is encrypted again this time with the public key of the Official user – it also contains a MAC code.

- It is formally stated as: \( \{^{\text{ENC}}\text{PK}_{ou}(^{\text{ENC}}\text{PK}_{uu}(\text{data})), ^{\text{MAC}}\text{SK}_{pd}\} \).
State of No Alarm (NA) (Illustrated)
State of Non-Critical Alarm (NCA)

- If the m-Carer detects a Non-Critical alarm condition, it sends an encrypted alert to the Location server.

- The location along with other data are sent from the patient's device to the Location server using a Non-Critical Alarm message that contains the data encrypted with a symmetric key \(\{K_{pd}\}\). A MAC is also added to the message to guarantee authenticity.

- Formally it is stated as: \(\{\text{ENC}K_{pd}(data), \text{MAC}SK_{pd}\}\).

- Upon reception, the Location server forwards the message to all users related to the patient. Then, users can decrypt the message, since they know the symmetric key \(\{K_{pd}\}\).
State of Non-Critical Alarm (NCA) (Contd.)

- Detection that a *patient* is located in a non-allowed area (marked in yellow) raises this alarm.

- These areas do not represent a direct risk to the safety of the patient, but the fact that the patient is there might indicate that he is lost.

- In this situation the m-Carer sends the message described above to the *Location server* that forwards it to Ellie and Mrs. Andrews (e.g. they receive a warning message in their mobile phones).

- They can decrypt the message because they know the secret symmetric key $\{K_{pd}\}$. After decrypting the message Ellie and/or Mrs. Andrews may act accordingly.
State of Non-Critical Alarm (NA) (Illustrated)
State of Critical Alarm (CA)

- If a critical situation is detected, it sends an unencrypted message to the *Location server* that forwards it to all users related to the patient.

- In addition, in parallel, the m-Carer sends a warning message to the *Emergency Services* informing about the location of the patient in clear text (i.e. no encryption is used).

- In this situation the safety of the *patient* is more important than his privacy, thus, the m-Carer automatically sends a warning message to the *Emergency services*.

- Also, the m-Carer sends an unencrypted message with the location of the *patient* to the *Location server* that immediately forwards it to relatives and caretakers. They will receive the warning in their mobile phones - in addition, the system can automatically make a distress voice call to warn them more reliably.
State of Critical Alarm (NA) (Illustrated)
State of Critical Alarm (Illustrated)
Obtaining Information

- Depending on the alarm state, the m-Carer encrypts the location information differently.
- If the message is sent under the Critical Alarm state, no encryption is used - users receive the information in plain text and no further action is required on their side.
- In a Non-Critical Alarm state, messages are encrypted with a single symmetric key known by official and unofficial users related to the patient.
- Only these users will be able to decrypt the message. The Location server that stores and forwards the messages is not able to decrypt them – then the privacy of the patient is fully guaranteed.
Obtaining Information (Contd.)

- For messages encrypted during normal operation (i.e. in a No Alarm state), official and unofficial users have to collaborate to decrypt the information.

- Neither official users nor unofficial users are able to obtain the information individually. Thus, the privacy of patients is guaranteed.

- Ellie is worried and wants to know the location of her father. She contacts Mrs. Andrews and asks for her help to determine the location of Mr. Oldsmith. If they agree, Mrs. Andrews starts the decryption procedure by using her private key and sends the partially decrypted message to Ellie. Ellie receives this message and finalizes the decryption using her private key and obtaining the location of his father.
Obtaining Information (Illustrated)

Flowchart:
- **Idle**
  - Get location & data
  - **State**
    - NA
      - RSA
    - NCA
      - 3DES
    - CA
      - Plain
  - Send signed message to location server
Conclusions and Future Work

- The number of people with mild cognitive impairment grows and it will keep growing in the future due to the aging of our society. Most of these people are able to carry a normal life, however, they can get lost or disoriented in some occasions.

- In these situations, they could be injured and finding them rapidly is very important. Although there exist some proposals to locate people, none of them fully considers the privacy of the user. Thus, this lack of privacy protection might prevent patients from using these systems.

- There is a clear need for new proposals able to balance the right of patients to be properly treated and controlled and their fundamental right to privacy.
Conclusions and Future Work (Contd.)

- Integration with indoor systems: The concept of m-Carer is basically designed for outdoors (due to the constraints of GPS receivers). Thus, integrating m-Carers with indoor monitoring systems would lead to a comprehensive solution.

- Cellphone loss: Depending on the stage of the illness, patients might lose their cellphones. Determining the best way of carrying the cellphone to avoid its loss is still an open issue.

- Wandering detection: Patients can get lost within allowed areas, in this situation, the system would not detect any alarm. It is desirable to develop methods to determine whether a patient is wandering even within safe areas.
Questions?

Feel free to ask anything!