Constrained Data Transmission with Critical Services in Healthcare

Sajida Zouarhi
LIG, Grenoble INP, HADAS team - ORANGE LABS
sajida.zouarhi@orange.com
28, chemin du vieux chêne - BP 98 - 38243 Meylan Cedex, FRANCE

Introduction and facts

Transmission of constrained data is a major issue in industrial systems. Today, we find more and more sensitive data in circulation. Regarding the transmission channel, questions of security, confidentiality, but also end-to-end integrity and traceability are hot research topics. It is of course a major concern in healthcare, especially in telemedicine where telecommunications are used to enable tele-expertise or tele-monitoring services. We qualify these type of services as *Critical Services* because they transmit *Constrained Data* with specific needs in QoS such as end-to-end guaranteed transmission time, privacy etc. In Healthcare, some threats are even more specific [1]. Health data are very sought after by cyber-criminals for blackmailing, spying and monetizing. Nowadays, a social security number is worth more than a credit card number [2].

The world is becoming a connected place. With the IoT coming, Healthcare will not be spared, which is why it is important as of now to understand and anticipate the risks that come along with this transformation.

First we will present a use case in healthcare to illustrate the problem in a concrete way. Then we will introduce the approach that we propose to better understand and define *constrained data* and *critical services* with examples. Finally, we will briefly describe the future work and conclude on some considerations about constrained data transmission through critical services in Healthcare and beyond.

Use case in Healthcare

The current trend in aging population will result in an increase of chronic diseases (i.e. cardiovascular diseases, diabetes, respiratory diseases and kidney diseases). In this context, telemedicine can improve the management of these illnesses by using information and communication technologies. [3]

In the world of tomorrow, hospital services will be decentralized. It will be possible to monitor a patient outside the hospital - at home or in mobility. People leaving in remote location will have a fair access to health services and new kind of decentralized use cases will emerge.

The digital transformation of health will be social – more regular follow-ups, more comfort for the patient, fair access to health service - [4], economic – reduction of the costs, see the report [5] - and ecological – fewer unnecessary travels. To support this transformation, telecommunication networks and information systems will have a major role to play, hence our focus on data transmission system.

Here is a simple use case illustrating a tele-monitoring situation. Alice is a patient suffering from a chronic heart disease and she needs very regular follow-ups with her Dr. Bob – see *figure 1*.

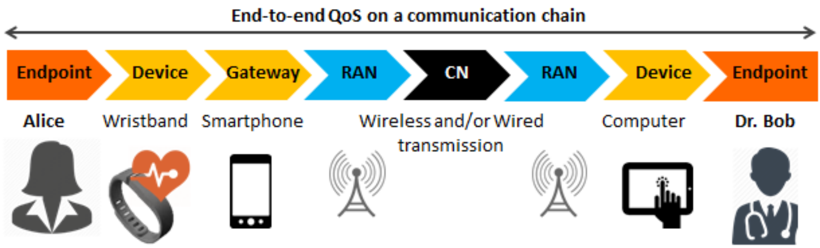

Figure 1 – End-to-end communication chain

If we use this communication chain, we automatically expose very sensitive data about Alice’s health and identity to risks (e.g. security breach because of an attacker, transmission delay due to traffic congestion).

Being able to guarantee privacy, integrity, traceability, time and delivery of the data all the way is really challenging. This is why we need critical services to handle in a proper manner the transmission of such constrained data.

Proposed approach

Our motivation is to be able to guarantee the end-to-end QoS on a communication chain from sender to recipient. We want to help design appropriate critical services for constrained data transmission through a decision support platform.

Constrained data. Type of data that require a critical service for a safe and reliable transmission.

Critical service. Transmission service which provides fine-grained end-to-end QoS with respects to data’s constraints. A CS is supported by a communication chain which failures (hardware or software) or lack of QoS could lead to serious consequences for: the end users (Alice & Bob), the service provider (Orange) and the client of the service (Hospital).

Here is a non-exhaustive list of constrained data to provide some concrete examples:

Health data	**Sensor data**	**Identification data**
vital measurement, documents (pictures, MRI scan), personal health record (allergies, disability, blood tests)	GPS position, accelerometer T°, humidity, pressure	name, ID card number, social security number

Figure 2 – Constrained data examples

We often find the term "critical data" in industry or technical literature. However our research shows that the criticality is not inherent to the data, it is related to **how the data should be transmitted** by a service, hence the use of the terms *critical service* and *constrained data*.

If we consider this subtlety, we can know define precisely the QoS constraints $\boldsymbol{C_{QoS}}$ of a critical service quantitatively and qualitatively with respect to the need $\boldsymbol{N_{service}}$ that the user expressed which is very useful for modeling.

$$\boldsymbol{N_{Service}} \rightarrow \boldsymbol{C_{QoS}}$$

Indeed, if one wants to design critical services in an automatic way, it is interesting to be able to formalize precisely how the Need expressed by the Client (e.g. a hospital that wants to use Orange Critical Service to deploy a new tele-monitoring service for its patients) impacts the Constraints on the Service in terms of **SLA** (service level agreement). In our work, we consider five main **Constraints criteria** for our QoS model:

$$\boldsymbol{C_{QoS}} = (Privacy, Integrity, Traceability, Delivery, Time)$$

The presence of a cross « X » indicates a specific need that is more than « best effort » or standard QoS level. (X) between brackets means that it is not a priority but it eventually depends on the use case. A bold **X** means that this constraint is crucial for this type of critical service

Type of Critical service	**Privacy**	**Integrity**	**Traceability**	**Delivery**	**Time**
Simple *collection*		X		X	
Active *monitoring*	(X)	X	X	X	X
Passive *monitoring*	X	X	X	X	
Continuous	(X)	X		X	**X**
Discrete	(X)	X		X	(X)
Actuator		**X**	X	X	(X)

Figure 3 – A mapping of critical services

Simple data collection. Messages are transmitted with two strong requirements: being delivered with a notification of success for the sender, and providing a high integrity. Any corruption of the data by a malicious entity or because of a problem in the network is unacceptable because these data might be used for patterns detection or knowledge inference.

Data monitoring. *Collection* means that the transmitted data are stored for a later use, whereas *monitoring* indicates that the data are used as they arrive by the end-user (or the application) for visualization, computation on-the-fly, or decision making in real time.

Active VS Passive. In an *active* critical service, the data can trigger an **alert** (e.g. rescue teams are notified) whereas a *passive* critical service has no action directly linked to it, hence no real time requirement

Continuous VS Discrete. A *continuous* transmission refers to a critical service transmitting a data flow with a very high sampling frequency which means that any small delay can directly affect the QoS of the critical service, as opposed to *discrete* transmission (e.g. one measurement per minute).

Actuator. In this type of critical services which is by definition *active*, the data can directly trigger a sensitive action on the endpoint (e.g. change the parameters of a pacemaker from a remote location, inject insulin to the patient), this type of CS requires high QoS because any mistake or security breach can lead to serious damage for the patient.

If we take our previous use case (Alice → Bob), the Need ($\boldsymbol{N_{Service}}$) is to design a critical service that can monitor Alice's heart with an alert system in case of abnormalities detection.

The *reasoner* component of our *Core* system will be able to match the Need of the User with the Constraints and compose a suitable critical service (CS) like this one and infer the proper SLA:

$$\boldsymbol{CS_{A\rightarrow B}} = \{\ active \wedge\ monitoring \wedge discrete \wedge real\ time\ analysis\ \}$$

Future work

We will complete the definition of the links between Need, CS and SLA. The next major axis in our research will be the implementation of our ontological model for the decision support platform. Our platform will be domain-agnostic (any domain with constrained data is concerned) while being specific enough to handle heterogeneity and complexity of the need at a fine-grained level. Our solution aims at modularity and evolutivity. For this reason, adding new types of a *constrained data*, or increasing the *knowledge database* with various models – physical or statistical – and rules is possible, without having to change the *core* algorithms.

Conclusion

A new world of opportunities and challenges is opening up before us. Healthcare is a good illustration of why guaranteeing QoS for constrained data transmission is crucial. However the concepts brought here are cross-cutting for different fields (smart home, smart city, finance, crisis management etc.). In this short paper we were able to give insights about *constrained data* and *critical service,* and highlight the relevance of such terms. As a quick overview, we also explained our approach which consists in a decision support platform to help design fine-grained critical service.

References

[1] TICsante.com, «Fuite de données et tentatives de chantage à la Clinique de Champagne,» 2012. [En ligne]. Available: http://www.ticsante.com/Fuite-de-donnees-et-tentative-de-chantage-a-la-clinique-de-Champagne-NS_1280.html.

[2] A. Beky, «Pourquoi les hôpitaux US sont dans la ligne de mire des hackers?,» 2014. [En ligne]. Available: http://www.silicon.fr/hopitaux-us-hackers-community-health-96181.html.

[3] P. Finet, R. Le Bouquin Jeannès, O. Dameron et B. Gibaud, «Review of current telemedicine applications for chronic diseases. Toward a more integrated system?,» vol. 36, n° %13, 2015.

[4] C. Charasse, «Télésurveillance et télé-expertise en Hémodialyse : expérience de télésurveillance de Saint Brieuc,» 2001. [En ligne]. Available: http://www.soc-nephrologie.org/PDF/epart/industries/gambro/2013/01-charasse.pdf.

[5] Ministère de la Santé et des Sports, «La place de la télémédecine dans l'organisation des soins,» 2008.

Author’s info

Sajida Zouarhi is an engineer and a PhD Student in Computer Science and Network since 2014 with Orange Labs and LIG (computer science laboratory of Grenoble). The work presented here is related to the following thesis subject: “***Quality of service of complex and heterogeneous systems for critical data transmission***”.