Mobile Peer-To-Grid Architecture for Paramedical Emergency Operations

Andrew Harrison a b Ian Kelley a b Emil Mieilica c Adina Riposan c d,1 and Ian Taylor a b

a School of Computer Science, Cardiff, UK
b Center for Computation and Technology, LSU, USA
c Contact Net Ltd, Bucharest, Romania
d Department of Applied Informatics, Military Technical Academy

Abstract. In this paper we describe a distributed architecture that could be used to link emergency medical centres, hospitals, telephone operators, and ambulances into a hybrid Peer-to-Peer (P2P) and Grid system for the sharing of information and transport of data. Distributed computing techniques can be used to connect static and mobile systems, bringing the different tools, expertise and databases together to aggregate patient data “on-the-fly” and then integrate it into a situation and context-specific patient-centred virtual environment. The scenario presented in this paper encapsulates connecting mobile tools and medical devices from ambulances, enabling data transfer to medical centres, and aggregating patient data from numerous sources. The proposed P2G (Peer-to-Grid) framework consolidates Peer-to-Peer and Grid computing research by addressing the mobility of transiently connected devices while supporting interactive configurability of components for dynamic data-driven distributed paramedical scenarios.

Keywords. Grid P2P WSRF Mobile WSPeer Medical Paramedical Emergency

1. Introduction

Recent advances in Grid [3][14] and Peer-to-Peer (P2P) technologies [10][11] now enable the research community to begin exploring how these systems could be adapted towards improving the current operating procedures of common yet difficult problems that persist in our day-to-day lives. The health care field is one such area, which due to its distributed nature of hospitals, emergency centres, and ambulances, combined with its high security requirements regarding sensitive patient data, matches well to what could be accomplished using a hybrid Grid/P2P infrastructure.

By combining Grid and P2P systems [5], an intelligent and context-aware distributed architecture can be developed that would dramatically increase the amount of information available to paramedical teams as they respond to emergencies, as well as improve information exchange with hospitals, emergency dispatch centres, and doctors. This information would range from patient data such as allergies and current medical condi-

1Email: adina.riposan@contactnet.ro, Web: www.contact-net.ro
tions to infrastructure related decisions such as traffic advisories and the relative proximity of hospitals with adequate medical facilities. By forming an effective and well-administered ambulance and fleet-management system that interconnects with medical centres, an emergency institution’s capacity to respond to crisis in a timely manner is greatly enhanced. In addition, once such a system is in place, it facilitates interoperation and communication with other government entities such as the fire brigade, police force, and public defense institutions.

As Grid computing has evolved, the field has moved towards service-based architectures, similar to web services [15], in the form of specifications such as the Open Grid Service Architecture (OGSA) [4]. With the move towards standards that promote service interoperability like WS-RF [3][9], it is now becoming possible to apply common techniques to different application and technology domains to create hybrid systems.

In this paper, we present how such a hybrid framework of Grid and P2P, which we call P2G (Peer-to-Grid), could be used to address the issues of a real paramedical emergency scenario. The move towards P2G represents a shift in paradigm from two perspectives: it addresses the seamless integration of mobile and static distributed resources, incorporating solutions to enable true mobility and transient connectability of such devices; and it supports the run-time integration of components and data through service orientation and dynamic discovery.

This paper is organized as follows: Section 2 introduces the medical support system; Section 3 describes ambulance fleet-management; Section 4 outlines the overall system architecture; Section 5 defines the security implications. Section 6 concludes the paper.

2. Paramedical Emergency Support

In this section we introduce the medical infrastructure involved in P2G emergency operations. To show how these infrastructure components could work together, a scenario is presented which details the step-by-step process that would take place from the moment an emergency call is placed until a patient arrives at an emergency centre.

2.1. The Medical Infrastructure:

Here, we describe the different types of participants and core facilities which are available within the scope of our scenario. These include static entities, such as the emergency control centre and the medical units, as well as mobile entities, such as the ambulances and portable medical devices, which need to communicate patient information on-the-fly when necessary. The static entities we have identified are listed in the following:

- **The Medical Emergency Control Centre** is a paramedical control centre that acts as the management and monitoring authority for emergency operations.
- **The Medical Data Resource Centres** are the medical units or hospitals that record patient data (keeping health records databases). These centres provide patient data to the infrastructure during an emergency if health records or other patient-data are necessary and available for discovery.
- **The Medical Emergency Units** are the medical units or hospitals that are accepted and acknowledged as Emergency Medical institutions where emergency patients can be transported. The selection of a Medical Emergency Unit for a
particular situation is based upon factors such as proximity to accident, available space, medical expertise and the specific health requirements of the patient.

The Medical Data Resource Centres and the Medical Emergency Units may or may not be the same during a particular paramedical emergency operation. Medical units are assigned initial roles in the infrastructure, but it is expected that many will be able to function as both patient data resource providers and emergency units, making their role in a particular situation case-specific. The Emergency Control Centre itself may play any or both of these roles.

Beyond providing basic access to medical data and patient health records, virtually all the medical units can play the roles of knowledge providers or resources, giving access to expert opinions and linking to more advanced situation analysis tools. Emergency operations in these scenarios are highly dependent on ensuring that the required information is delivered in real-time and supported by expert assessments with the assistance of teams from the Medical Emergency Control Centre as well as other participating medical units. Therefore, static entities in the emergency infrastructure ensure adequate management and monitoring functions, as well as providing a Data and Knowledge Access point to mobile entities. The Mobile Entities within this scenario include:

- **The Fleet of Ambulances** are managed and monitored by the Emergency Control Centre to maintain both mobility and automatic navigation requirements in emergency operations, as well as communication and data transfer among different participants within the infrastructure and data transmission between the paramedical mobile devices and the virtual emergency environment.

- **Medical Devices** which consist of the various types of mobile devices used in ambulances that can potentially record real-time data from patients. Such medical tools and equipment can be used for ad hoc medical data acquisition, initial patient diagnosis and monitoring of the patient’s current medical condition during transit to a hospital facility. Specialised software and tools are used for the acquisition and quantification of the patient’s vital medical data, using monitoring sensors for the monitoring of the body functions and parameters, which is subsequently transmitted to other entities involved in the emergency operation.

- **Personnel Devices** are mobile devices which are used to communicate with participating individuals such as paramedics and ambulance drivers.

2.2. A Paramedical Scenario:

In this section we present a scenario of how the interactions between the Medical Infrastructure entities are managed within real-world scenarios that integrate the static and mobile entities to potentially automate the medical planning process within an emergency situation.

2.2.1. Initiation and Monitoring of the Emergency Operation

When an emergency call is received by an Emergency Control Centre operator, he/she performs a primarily analysis and makes the decision to initiate an emergency operation. A Virtual Emergency Environment (VEE) [1] is created to dynamically integrate the appropriate patient-related data from both the medical units that are currently treating and monitoring the patient (static data resources) and the medical diagnosis tools in the am-
bulance during the patient’s initial examination and transportation to the hospital (mobile data resources). Ambulances are selected based upon proximity to the emergency and are dispatched to the emergency site, with the mobile-grid fleet management system ensuring proper directions and automating the navigation-specific functions that are necessary, thereby providing more reliable response service over large geographic areas and high-risk locations (see Section 3). In more complex rescue operations, this system would be able to interface with other intervention units such as the fire brigade or police force.

During the initial patient analysis, raw data is acquired from the scene by the paramedical team and transmitted to the Emergency Control Centre, which monitors operations and maintains communication with the ambulance’s paramedical team. In some cases, the emergency operation is supervised and assisted by experts during the initial examination, diagnosis, and transportation to the medical emergency unit. This could potentially involve specialists from several hospitals, requiring the interactive communication and data transmission among all the actors and knowledge sources to be integrated within a Virtual Emergency Environment (VEE). By calculating factors such as the initial diagnosis, the distance to travel, and available bed space, an appropriate hospital is chosen by conducting a search of available resources. The casualty unit in the selected hospital is notified and is provided with access to the patient’s medical records.

2.2.2. On-site Emergency Management

We envisage an emergency scenario for complex and high-risk situations that requires the presence of several ambulances to conduct the rescue operation, potentially in large areas and high-risk environments. For such cases, one must take into account not only the permanent communication channels with the Emergency Control and Data Centres, but also local communications between on-site entities involved in the operation, such as the fire brigade and police force.

In the ambulance environment there are a set of mobile devices (medical devices and personnel devices) that communicate with each other and exchange data locally during the rescue operation. For example, the personnel mobile devices receive notices and automatic messages from the medical tools and sensor devices that permanently monitor the patient state and perform ad-hoc vital data acquisition from the patient. A controller node is situated in the ambulance and acts as a gateway to the ambulance environment, handling data transfer to other ambulances participating in the rescue operation, and to the Emergency Control Center. The controller node could either be integrated into the ambulance itself or added to the vehicle as a separate device (see Section 3).

Mobile device communication via a controller node (the ambulance) is unnecessary for the internal communication within the ambulance environment, however, we consider it necessary for the communication with the other ambulance environments and the Emergency Control Centre. One important reason for such necessity is the security and data privacy requirement regarding patient data that is published into and received from the Virtual Emergency Environment. Although trust relationships may exist between the mobile devices participating in the local ambulance environment, for outside communication and data exchange with the VEE there are additional authentication and authorization requirements. This additional security layer would be handled by the controller node, using the local authentication and remote authorization system of the ambulance
A. Riposan et al. / Mobile Architecture for Paramedical Emergency Operations 5

(see Section 5), in connection with the communication interface of the vehicle (see Section 3).

The ambulance itself plays an important role in maintaining mobility, coordination, and automatic navigation requirements in emergency operations. The fleet management system automatically ensures direct communication between the ambulance’s controller node and the Emergency Control Center, as well as coordinating on-site communication with the other ambulances and rescue participants (fire brigade and police force) (see Section 3).

In order to achieve fault tolerance in the case where a controller node fails or becomes unavailable, we envisage the capability to automatically transfer the coordination and management functions to another mobile entity. In this event, the responsibility for publishing data into, and receiving support from, the VEE would be transferred to another mobile device(s) in the ambulance environment, such as personnel devices that have the required technical capabilities.

2.2.3. Data and Knowledge Access

Within the paramedical emergency infrastructure, data and knowledge resources can be highly distributed. These resources need to be combined into an Emergency-centric Grid-based virtual environment in order to ensure patient-centred rescue operations and medical care. Patient medical data resides in health records repositories hosted at different hospitals and medical units where patients are currently being treated and monitored. Mobile units such as ambulances need to discover the Medical Data Resource Centres and locate the available health records by using available information about the patient in order to integrate the required data and create the patient-centred VEE. The data and knowledge resource discovery can be achieved by performing a decentralised search across the P2G network super-peers or hubs, thus maintaining both the dynamism and robustness of the network.

The type of information available can range from simple identification, e.g., a driving license, to the use of a patient’s Electronic Health Smartcards / Health Insurance Smartcards if available. Such cards can provide information about the medical units keeping health records connected to the patient under consideration, thereby helping in the distributed search. They also provide immediate access to vital data and the medical history of the patient, which can be easily integrated in the virtual emergency space of the patient and support the decision making process. Patient identification through the use of electronic health smartcards or health insurance smartcards can be achieved using local authentication to the ambulance facilitated by the communication interface in the vehicle and remote authorisation using GSI (see Section 5).

2.2.4. Creating the Virtual Emergency Environment

At the Emergency Control Centre, a VEE can be automatically constructed. This is where all information needed for the optimum care of the patient is made available (as described in [1]). In our case, such information can be accessed through standard searching mechanisms offered within the P2G architecture. A first responder (e.g., an ambulance driver) can be granted access rights for the VEE and can communicate with other participants using standard voice over IP (VOIP) or even video technology.

Specialised software for the acquisition and quantification of a patient’s vital medical data and monitoring sensors for the monitoring of the body functions and parameters
can be used as initial ambulance diagnosis tools. Enhancing the use of specialised amb-
bulant radiology tools to perform radiology examinations by using mobile MRI or CT
could increase even more the usefulness of this scenario. The current patient’s condition
during travelling to the hospital can be communicated to the VEE. The sensors and the
software operators for sensor data acquisition are gathering the patient’s medical and
physiological parameters, biometric and environmental data. This setup will allow for
unobtrusive monitoring of electrocardiogram (ECG), heart and respiratory rates, blood
pressure, blood glucose level, oxygen saturation, skin temperature, etc. Sensors can be
integrated via base stations and pre-processed locally. Filtered signals and data are in-
stantly transmitted to the Emergency Control Centre and integrated within the VEE. All
medical and physiological measurements become thus available, via the gateway. Fur-
ther, as described in [1] a Virtual Emergency Health Record (VEHR) could be created.

3. Ambulances Fleet Management:

The fleet management application for the effective automatic administration of the fleet
of ambulances can be interfaced for end users by a specific fleet management portlet
integrated into the Portal. A Web-based portal can be customised by any organization
hosting the Medical Emergency Control centre for administering the services provided
by the proposed infrastructure. The portal facilitates the sharing, distribution, adaptation
and evolution beyond the state-of-the-art in fleet-management. The system allows the
vehicular mobile Grid nodes to monitor their environment, record changes and react
intelligently in a dynamically changing environment. Currently there are a number of
proprietary systems that have attempted to tackle the issue of fleet management, but
largely have ignored the important areas of:

- **Integration with onboard equipment and in-vehicle environment:** there is a
  pool of information available about the internal state of the vehicles that can be
  used for better decision making both for the driver and for the management or ad-
  ministrator of the fleet of Ambulances. Mobile agent can constantly monitor and
  record this data and take decisions or generate reports based on these recordings.
  Further integration with onboard systems, such as the sound system, will provide
  the basis of a better, more secure way to interact with the driver.

- **Interoperability with other systems:** core new services and capabilities can take
  full advantage of the benefits the Grid has to offer: interoperability, dynamic use
  and discovery of resources, ubiquity, composability of services, security, notifica-
  tion, collaborative working, data handling, and remote visualisation.

- **Availability on a wider geographical area:** intelligent mobile agents can adapt
  to the changing environment including variations on the availability and Quality
  of Service (QoS) of accessible mobile data carriers. Such agents can choose the
  appropriate means of communication by analysing available bandwidth, predicted
  latency, cost, etc.

4. System Architecture

The scenario described in Section 2 poses specific challenges for a system architec-
ture. In particular the integration of static, computationally powerful infrastructures with
lightweight, mobile and potentially transient devices must be addressed. A core require-
ment of the system is that it handles the limitations and heterogeneity of the mobile
network and negotiates between this network and the static Grid. Negotiation responsi-
bilities should include translating between the static Grid and the mobile network, for
example security contexts, and maintaining connectivity and location transparency of
mobile nodes. Furthermore mobile devices require a network infrastructure that allows
them to discover, and relay data and messages to other nodes. This infrastructure must
support node unreliability, that is, handle changes in transport and dynamic network path
configuration.

To enable the integration between static and mobile Grids we believe there are two
important concepts that should be adhered to. Firstly that the system should be loosely
coupled and secondly that this loose coupling should be supported by a common mes-
saging framework. By designing the system around the Open Grid Services Architec-
ture (OGSA) and it’s current incarnation - The Web Services Resource Framework (WS-
RF) [3] - we believe this can be achieved. WS-RF allows systems to combine service
orientation with standard SOAP message exchange patterns. In particular WS-RF al-
 lows the de-coupling of resources exposed via services (called WS-Resources in WS-RF
parlance) from the service that exposes them. In a resource intensive environment as is
described, this is essential to maintain a loosely coupled system.

4.1. Mobile P2P Grids

The requirement of negotiating between networks can be addressed through a three lay-
ered architecture which connects the static Grid with the mobile network via a bridging
layer. This bridging layer needs to able to face two ways, that is, it must be capable of
handling both the security, service and transport infrastructure of the static Grid and of
the mobile network. Figure 1 depicts this three-layer design. In this architecture mobile
nodes communicate directly with the bridge layer which in turn communicates with static
Grid entities such as hospitals and patient record databases. Here the bridge layer acts
as an aggregation service for the various devices in the mobile Grid. This architecture does not address certain requirements of the scenario however. In particular it does not allow local discovery and decision making. For example, if patient data is required on site, this needs to be retrieved by each node that requires it from the bridge layer. This in turn hinders scalability because all communication must go via the bridge layer and hence it is in danger of becoming a bottleneck to the system.

The requirement for mobile nodes to communicate directly with one another, as well as the ability for the on-site communication model to scale to any number of ambulances and other mobile emergency teams such as the fire brigade requires an approach that allows nodes to act as both service providers and consumers that can discover one another in a decentralized manner - that is a Peer-To-Peer (P2P) system. Furthermore the structure of ambulance environments and the security requirement for controlling access to the bridge layer from within these ambulance environments suggests a centralized/decentralized system such as a super peer architecture. Other projects that address Grid and mobility do not directly consider the topology issue. The Mobile OGSI.NET [16] system does not address discovery or topology at all, concentrating solely on exposing mobile devices in an OGSA compliant manner. Similarly the Akogrimo [1] project delegates discovery and topology to a variety of protocols. We consider the introduction of a super peer architecture to handle controlled yet scalable interactions between diverse nodes a significant development in mobile-to-static Grid infrastructures. Figure 2 depicts the design we call Peer-To-Grid (P2G) which extends the architecture depicted in Figure 1 by enabling groups of peers to interact directly with one another within their group (the ambulance environment in our case) and for these groups to interact with each other and the bridge layer via a super peer (the ambulance controller node in our case).

The implementation design of P2G is based on the Web services framework called WSPeer [8]. WSPeer is an API focused on the cross-fertilisation of P2P and Web/Grid services. As well as supporting simple Web service interactions it is also capable of interacting with Grid middleware using WS-RF and related specifications. It allows easy inte-
migration of different protocols underneath the Web services technology stack and currently supports among others, a lightweight, domain independent framework capable of advertisement, discovery and communication within ad-hoc P2P networks called P2PS [11]. Like JXTA, P2PS uses the ‘pipe’ abstraction for defining communication channels. Pipes can traverse multiple transports and contain intermediary nodes. P2PS also uses logical addressing and endpoint resolver services for translating logical addresses to network specific addresses. This is particularly useful in handling host mobility and migration as it allows the logical address to remain consistent while the underlying location or transport changes. A subset of WSPeer functionality is currently being developed which allows mobile devices to communicate with each other using Web service and WS-RF messages over HTTP and P2PS. Using WSPeer allows us to implement the core functionality of system nodes as described in the following sections, in particular the ability to bridge different protocols and topologies and function in resource constrained devices while maintaining a standards compliant service interface.

4.2. Bridge Node architecture

Structurally we expect the bridge layer to be static and stable, much as the Grid layer is. The nodes that inhabit the bridge layer create a view of the mobile network that the static Grid can understand and a view of the static Grid that the P2P network can understand. Internally the bridge nodes must map between these views. We consider a proxy design pattern the most appropriate. Mobile nodes and groups are presented to the Grid via this proxy allowing the Grid to conceive of them as usual Grid entities. This architecture requires certain properties in the proxy which enable bridging between networks.

Firstly, the proxy should possess agent-like autonomy, as it may have to make decisions or send messages on behalf of a mobile node if the mobile node is unavailable and immediate action is required. This may require the caching of status information on the node or group in question. Secondly, to facilitate connectivity transparency, the proxy must be able to store messages received from the static Grid and pass them onto mobile nodes when they are available again. This capability also allows optimization of message transfer, enabling the messages, for example notifications, to be aggregated into a single message. Finally, the proxy should perform translation between contexts, for example translating from a group-based security infrastructure in the P2P network to a user-based infrastructure in the static Grid.

4.3. Mobile Node architecture

Based on the requirements of the scenario and the capabilities of WSPeer, we have designed a mobile node architecture depicted in Figure 3. A mobile node is made up of a number of modules that communicate with one another to facilitate the functionality required by the scenario.

1. The Service Layer defines the interface to the mobile node, that is the protocols and messages understood by the node. This is implemented as an OGSA (currently WS-RF) service interface. The services exposed by a node consist of three types. Two types are shared by all nodes; these are services which handle the migration of the service to another node and the establishment of data channels. The
third type are node specific services that depend on the nature and function of the node in the network.

2. The SOAP module parses and generates SOAP messages.

3. The Data Channel module accepts and generates usually binary data flows such as images of audio/visual streams. The details of how this module is connected to is defined at the OGSA service level. A typical data channel might be described as accepting (or expecting) a certain MIME type, whether the data is to be streamed and where, if anywhere, the data should be passed on to. The ability to set the input and output sources for the channel will enable the construction of workflows in which data is streamed directly from node to node without passing through a controller node.

4. The migration module handles the migration of the service layer and any state or data (WS-Resources) hosted by the node.

5. The P2P module provides information to the service modules about the network neighborhood and offers capabilities for discovering other mobile nodes and resolving logical addresses. These capabilities are exposed by the service layer as network compatible services.

6. The device module is capable of introspecting the device and returning relevant information required by the other modules. For example the location of the device may need to be exposed as an OGSA service, but may also be required by the P2P module to decide on the best transport to use for connecting to another node. The device module is also capable of describing the device as a WS-Resource. This resource is exposed via the OGSA service interface.

7. The protocol module handles different transfer protocols such as HTTP or Session Initiation Protocol (SIP). Protocols may be chosen directly by the P2P layer or passed to it from the service layer or data channel module.

8. The transport module handles the details of the network transport chosen by the P2P layer in consultation with the device module.
5. Security Infrastructure

The distributed system described here can be divided into two fundamental parts: a static set of Grid resources and multiple dynamic resource sets that will be created in an \textit{ad hoc} method, as needed, using secure P2P protocols [2] and services. This meshing of Grid and P2P systems requires that traditional security infrastructures be enhanced to support both environments in a seamless manner. This could be done either by extending current security mechanisms to support both systems or by using a "bridge" to link the networks together without modifying their native security infrastructures [12][7]. Regardless of the final implementation, the central concerns of authorization and data integrity will be the same – how to ensure correct access rights and integrity of data. It is therefore fundamental that when such systems are designed, and ultimately deployed, that security policies are established that can verify the identity of users and services, protect communications, and make intelligent decisions about what access rights a particular entity is allowed within the network.

The dynamic nature of fleet operations requires that users are able to create services “on the fly” without administrator intervention. These services must be coordinated and able to interact securely with other partner services. Therefore, the security infrastructure involved in these operations must be able to adapt to new services and users as well as be configurable to allow for multiple VOs and provide rich group membership information.

In addition, the nature of the mobile fleet requires a security infrastructure that can be used in the context of a system that requires disconnected operation. Local authentication functionality and remote authorization must be decoupled, allowing for nodes to appear and disappear off the network, yet still maintain a session between connections. This way, a mobile node can operate offline, storing secured tokens that are then reused for updates and synchronization operations when the mobile node is again online, without the need for classical authentication to the server.

Due to the mobility, time constraints, and stress factors involved in emergency operations, alternative end-user verification methods are required that go beyond traditional input mechanisms such as keyboards, which are prone to error and require a high level of user interaction. To address these issues, more portable and user-friendly technologies such as smart cards or biometrics are needed. In this scenario, certificate files provided by a smartcard device would be used to authorize local operations and, in connection with the communication interface of the vehicle, could be used to authorize the user to remote Grid infrastructure and services, allowing them to publish or receive vital medical information.

6. Conclusion

In this paper, we presented a combined Grid and Peer-to-Peer architecture for application to dynamic paramedical scenarios that involve on-the-fly connecting and communicating across a collection of distributed resources. The resources we described in this scenario can be static, such as the emergency control centre and the medical units through to the mobile entities, such as the ambulances, which need to communicate on-the-fly patient information when necessary. We described the real-world interactions between these entities and then described an infrastructure, called P2G, which addresses the various problems that such a scenario exhibits.
References