A. Nieto, and J. Lopez, "Security and QoS tradeoffs: towards a FI perspective", *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, pp. 745-750, 2012.
http://doi.org/10.1109/WAINA.2012.204
NICS Lab. Publications: https://www.nics.uma.es/publications

Security and QoS tradeoffs: towards a FI perspective

Ana Nieto, Javier Lopez
Computer Science Department
University of Malaga, Spain
Email:{nieto,jlm}@lcc.uma.es

***Abstract*—Motivated by the growing convergence of diverse types of networks and the raise of new concepts such as Future Internet (FI), in this paper we present an analysis of current research on the development of security mechanisms in a tradeoff with Quality of Service (QoS) mechanisms. More precisely, we pay attention to the Security and QoS problems in resource-constrained networks that are candidates to be an important part of the FI due to their proximity to the user or because of their contribution to the information society. We analyse the current state of the research on security and QoS in the integration of sensors, MANET and cellular networks, with the aim of providing a critical point of view, allowing us to assess whether it is possible that such integration of networks is both secure and efficient.**

***Index Terms*—Security; QoS; Future Internet;**

I. Introduction

The concept of Future Internet (FI) is concerned with the future interconnection of heterogeneous networks. In the generic FI scenario, where a wide variety of devices will be coexisting in different domains composed of a myriad of entities, security becomes one of the main issues to address. More precisely, in order to encourage the collaboration of those entities, it is necessary to conceive mechanisms for the secure data exchange among them. However, due to the broad participation expected and the coexistence of multiple domains, these mechanisms must take into account the quality of service (QoS) requirements; otherwise, we may produce highly secure systems though useless from the point of view of usability. Currently, a security failure or incorrect QoS requirements can affect the appropriate functioning of a network, but once the networks begin to fully interoperate with each other, the security and QoS problems will affect the correct behaviour of interconnected networks of different scenarios if necessary precautions are not considered beforehand. Moreover, although both security and QoS mechanisms are essential in the FI, security and QoS are inherent conflicting features. In fact, the issue raises because, while the security mechanisms generally involve operations that are resource-expensive and limit the resources' availability for the rest of the services in the environment, the QoS mechanisms try to optimize the use of those resources that are limited by the security mechanisms. But, as mentioned, in the FI both types of mechanisms must coexist because both are extremely necessary. Indeed, it is expected to seek a balance between security and QoS in order to build efficient, scalable and secure architectures that are able to make an optimal use of resources while maintaining the necessary security level.

The objective of this work is to analyse the current state of security and QoS interdependencies in the integration of resource-constrained networks. These types of networks are good candidates for being part of the FI because of their proximity to the user and their contribution to information society in general. Currently, there are several studies that deal with network integration but without considering explicitly the interdependencies of security and QoS requirements. In more detail, in this paper, we anlyse the current state of research in security and QoS for the integration of wireless sensor networks (WSN), mobile ad-hoc networks (MANET) and cellular networks, and we propose schemes for the integration of such networks in the FI.

The work is structured as follows. In Section II we analyse the state of the art for each of the technologies covered in the paper with respect to security and QoS. In Section III we propose a taxonomy of technologies based on QoS and security requirements for the identification of common features and interest among the technologies. This taxonomy supports the analysis carried out in Section IV, where we propose QoS and security schemes to FI network cooperation. Finally, in Section V we present the conclusions and future work.

II. Related work

Studying the impact that security mechanisms have on QoS in the scope of WSN becomes a challenging task [**?**]. Moreover, deploying security features into sensors that are connected directly to the Internet can be a daunting task[**?**]. In fact, the Internet opens the door to a large number of possible threats and sensors are resource-constrained devices, unable to implement complex security mechanisms. This could severely limit the lifetime of sensors and other devices with similar characteristics, and inevitably affect the QoS [**?**]. In particular, routing tasks are the ones that consume more energy [**?**]. This is also a problem for some security mechanisms based on distributed information systems. For instance, establishing a reliable trust system requires the exchange of data between various nodes of the network and it severely affects energy consumption. Paradoxically, the lack of security mechanisms can have negative consequences for QoS in WSN. Thus, Christin et al [**?**] shows that the lack of integrity in communication increases the packet loss and decreases the throughput. Moreover, without authentication mechanisms, a malicious node can impersonate other nodes in the network and affect the availability of the network. Besides, attacks to WSN that affect the performance are very difficult to distinguish from

perturbations in the network due to environmental conditions. For example, a storm could wipe out several sensors and then isolate the network, or the part of it that could be critical for data collection or their transmission. One interesting approach is to consider the QoS as a requirement for security in WSN (and vice versa). In that sense, availability is taken as a security requirement in several security studies [**?**][**?**].

On the other side, many MANET scenarios are composed of heterogeneous devices, making it even more difficult to establish QoS guarantees and to deploy security mechanisms. Most QoS models proposed for MANET are influenced by the protocols IntServ and DiffServ [**?**]. For example, Zouridaki et al [**?**] analyse the security threats in resource reservation (QoS signaling) in MANET, using the INSIGNIA and SWAN protocols based on IntServ and DiffServ, respectively. That work concludes that, regardless of the protocol, one of the problems is that reservation requests are accessible by any device with access to the transmission channel, that is of free access. It means that there are several devices that could identify these and other control messages and distort them or sabotage the resource reservation for their own benefit. Moreover, the device mobility makes it difficult to verify the legitimacy of QoS request, and the limited resources make the deployment of QoS monitoring techniques difficult. Along the same lines, the work [**?**] lists several security and QoS problems in MANET, but focuses on the intrusion detection mechanisms to detect and prevent QoS signaling attacks. In Hejmo et al [**?**] authors focus on defining the DRQoS protocol, a QoS signaling protocol for MANET resistant against some variants of flooding and over-reservation attacks. Furthermore, a particularly interesting feature of MANET is their ability for self-organization and the added advantage of being designed for highly dynamic scenarios. These factors have led to their study as networks to be deployed in critical situations. For example, Panaousis et al [**?**] define a framework for secure real time communications in MANET used for emergency rescue scenarios (e-MANET), by adding authentication of the sender, integrity and confidentiality (using IPSec), and by providing intrusion detection.

With regard to Cellular Networks, the majority of the studies based on 4G architectures highlight the approach All-IP on which they are designed, as well as their security problems and the need for QoS guarantees. Park et al [**?**] highlight the importance of dealing with attacks that affect to the performance and availability of cellular networks, such as Thelf-of-Service (ToS), Denial of Service (DoS) and IP spoofing attacks. In fact, these attacks can damage the service providers' reputation and this may influence the loss of customers. To avoid these and other threats, the security mechanisms must be strengthened, but without forgetting that the indiscriminate use of resources could itself become a threat to the whole system. In that sense, Shankar et al [**?**] proposes the combined use of elliptic curve cryptography (ECC) and symmetric key to address the vulnerabilities of a 3G-WLAN hybrid system. The IP-based mobility is also a hot topic in this area. For example, Fu et al[**?**] propose the architecture SeaSoS, which integrates QoS Signaling, AAA Services (Authentication Authorization Accounting) and mobility (in particular MIPv6) for 4G network infrastructure. SeaSoS also conceives the possibility that the end user or network operator can change the network attributes dynamically (eg. using HMIPv6 instead of MIPv6) in order to facilitate the interaction between heterogeneous networks. Along the same lines, Tiny SESAME[**?**] is a security mechanism based on dynamically reconfigurable components at runtime, so it is possible to add on-demand components and remove them if not needed at any given time. Moreover, Muraleedharan et al [**?**] highlight the need to provide QoS techniques adaptable to user needs and the importance of developing secure and efficient IP-based services.

The IP mobility schemes are also very interesting to consider for network integration. Indeed, several studies consider the use of MIP for 4G mobility management [**?**], while another ones choose MIH as an option to perform vertical handover[**?**][**?**]. In such studies both Security an QoS requirements are taken into account. Moreover, Pontes et al [**?**] considers that handover decisions should be based on several factors, among which we can find QoS and security support.

Finally, considering network convergence and interoperability between the above technologies, the coexistence of MANET and cellular networks is proposed in [**?**] and [**?**]. This alliance provides both security (due to the cellular networks infrastructure) and flexibility (due to the nature of MANET). Additionally, in the previously mentioned eMANET, the fast deployment of networks to maintain the communication between individuals allow their location or to assists them in the coordination of rescue services. So, the inclusion of WSN can help to prevent the rescue services suffering unnecessary harm (e.g. alerting about the risk of nuclear leaks in the case of a nuclear power plant). The integration of cellular networks and WSN is proposed by Mahonen et al [**?**], where they highlight the current and future contribution of sensors in industries (e.g. nuclear plants) or at home. In such approaches sensors would use cellular terminals as gateways for access to IP networks. Another approach is to consider the integration of heterogeneous wireless systems to offer a better service to the users (i.e. to be always-on, better connectivity)[**?**]. This point of view is very interesting because it increases the business opportunity for the service providers.

III. Taxonomy

We have analysed the taxonomy from two points of view. Firstly, the characteristics of each type of network are studied in order to find similarities between them (Table I). Secondly, we also have studied the requirements for network interconnection (Table II). As a first result, Figure 1 shows the parametric relationships between Security and QoS requirements.

On the one hand, Table I shows that, from the research works considered, the authentication and communication integrity are two properties repeated in most of the research works that address security issues, especially in cellular networks, where we must emphasize that there is a considerable increase in the importance of security services when compared

to the other two types of networks studied, being especially relevant the AAA Services. Regarding the QoS, in general the most studied parameter is the delay, followed by the bandwidth and the availability in MANET, while in WSN the energy consumption is the most relevant parameter, probably because it is key to calculate the network lifetime. In the particular case of the throughput in WSN, it is noteworthy that, although it is a parameter mentioned in several articles, is not discussed as thoroughly as the delay and the energy consumption. We must also note that the QoS signaling is analysed in several works related to MANET, where the analysis of DoS attacks also takes an important role.

On the other hand, Table II analyses the research works related with network integration. From this it follows that most of the works considered include QoS signaling (*QoS S.*), AAA Services (*AAA S.*) and the performance and security problems due to handover. Therefore, these approaches reflects the importance of deploying resource reservation and security mechanisms and ensure that such schemes do not adversely affect to the handover. Moreover, the deployment of AAA Services is necessary due to the cooperation among systems and the participation of users. However, there are several open issues here. Perhaps the most worrisome is the cooperation between mobile operators, since especially in these environments collaborative AAA Services must be deployed to allow the users monitoring, and to ensure the correct use of the network. Those services that allow QoS signaling must be deployed too. Moreover, the traceability or misuse of user's data must be avoided. Meeting both requirements is complex, especially if we consider several domains.

Finally, we define the dependency relationships between the parameters a and b as positive (D^+), negative (D^-), complete (D^c) and total (D^t):

$$
\begin{aligned}
&D^+ :: aD^+b \Rightarrow (\Delta a \rightarrow \Delta b)\\
&D^- :: aD^-b \Rightarrow (\Delta a \rightarrow \nabla b)\\
&D^c :: aD^cb \Rightarrow (\Delta a \rightarrow \Delta b) \wedge (\nabla a \rightarrow \nabla b)\\
&D^t :: aD^cb \wedge bD^ca
\end{aligned}
$$

D^+ means that the increment of the first parameter also causes and increment of the second parameter, whereas with D^- the increment of the first parameter causes the decrement of the second parameter. D^c means that both parameters are related positively and also the decrement of the first parameter affects the second parameter by decreasing its value. D^t means that the complete dependence is symmetric to both parameters.

Figure 1 shows the dependencies between performance parameters (orange ingot, e.g. availability), security properties (green square, e.g. integrity), characteristics of the environment (blue, e.g. to be a real-time system) and some consequences (gray hexahedron, e.g. collisions). Some lines are numbered indicating the relevance of such dependence regarding the rest of numbered dependencies with the same destination node. For example, delays can be more harmful than packet loss in real-time systems.

In general, real-time services require low packet loss and low delay in data transmission. The throughput might be

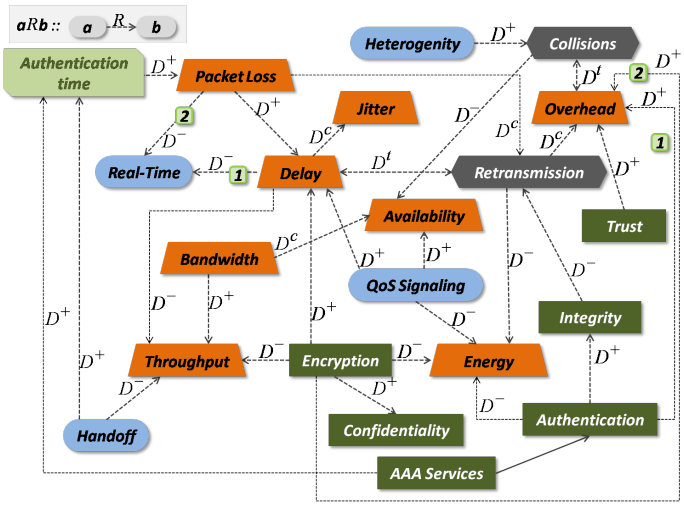

Figure 1. Parametric dependencies

relevant, but once we have the two characteristics above. Moreover, the throughput may be adversely affected by roaming scenarios, where hardening or relaxing the cryptographic mechanisms could affect it negatively or positively respectively. This parameter is influenced by the network bandwidth, which also affects the availability. Furthermore, the relationship between the QoS signaling and the availability should be nuanced. The QoS signaling mechanisms gurantee availability because they are used for resource reservation, ensuring the availability of resources for a service for a period of time. The downside of resource reservation is that requires the exchange of additional control messages and this entails an energy consumption that may be harmful to some networks. Also, the authentication mechanisms may require the exchange of messages, and the encryption mechanisms can increase the packet size to a fixed length regardless of the data length. Furthermore, the execution of cryptographic operations adversely affects to the energy consumption. However, the authentication mechanisms can provide message integrity, thereby avoiding the data retransmission and network overload. Moreover, the more overloaded a network is, the more likely to suffer collisions. In heterogeneous networks, collisions can occur more frequently when devices share the same communication medium. In addition, collisions damage the availability by avoiding the use of the medium for data transmission. The collisions are independent of bandwidth, as there are conflicts due to the simultaneous data transmission from various sources causing interference with each other.

It is important to note that Figure 1 is a simplified map that does not cover all the possible parameters, properties and features that we can find in each different network. To cover all these possibilities the resultant scheme would be even more complex than that. This gives us an idea of the difficulty of developing security and QoS tradeoffs mechanisms in heterogeneous systems, and maybe what is more important, the quite plausible risk of making a decision that affects several parameters and properties due to dependencies.

Paper	Security								QoS									Purpose		Type
	Authentication	Authorization	Integrity	Trust	Encryption	Key	AAA S.	IPSec	Delay	Throughput	Jitter	Bandwidth	Packet Loss	Overhead	Energy	Availability	QoS S.	Attacks	P. Analysis	
[?]	-	-	-	-	x	x	-	-	-	-	-	-	-	x	x	-	-	-	-	WSN
[?]	x	x	x	-	x	-	-	-	-	-	-	-	-	-	x	x	-	x	-	
[?]	-	-	-	-	-	-	-	-	x	x	x	x	x	-	x	x	-	-	x	
[?]	x	-	x	x	x	-	-	-	-	x	-	-	x	x	x	-	-	x	-	
[?]	x	-	x	x	x	-	-	-	x	x	x	-	x	x	x	x	-	-	x	
[?]	x	-	x	-	-	x	-	-	x	x	-	x	-	x	x	x	-	x	x	
[?]	x	-	x	x	-	-	-	-	x	-	x	x	-	x	-	x	x	x	-	MANET
[?]	x	x	x	x	x	x	-	-	x	x	x	x	x	x	x	x	x	x	x	
[?]	x	-	x	-	-	-	-	-	x	-	-	-	-	-	-	x	x	x	-	
[?]	x	-	x	x	x	-	-	x	x	-	-	x	-	x	-	x	-	x	-	
[?]	x	-	x	-	-	-	-	x	x	x	x	x	-	-	-	-	-	x	-	
[?]	x	x	x	x	x	x	x	-	x	-	-	-	-	-	-	-	x	-	-	Cellular
[?]	x	-	x	-	x	-	x	-	x	x	-	-	x	x	-	-	-	x	-	
[?]	x	x	x	-	-	-	-	-	x	x	-	x	-	-	x	x	-	x	-	
[?]	x	x	x	x	x	x	-	-	x	-	-	x	-	-	-	-	-	-	-	
[?]	x	x	x	-	x	x	-	-	-	-	-	x	-	-	-	x	-	-	-	

Table I
CLASSIFICATION BASED ON FEATURES

Paper	Technologies						Type					
	WSN	MANET	Cellular	MIP	MIH	Others	Integration	Attacks	QoS S.	AAA S.	Handover	Analysis
[?]	-	-	x	x	-	-	x	-	x	x	-	-
[?]	-	-	x	x	-	WLAN	x	-	-	x	x	-
[?]	-	x	x	-	-	-	x	x	x	x	-	-
[?]	x	x	x	-	-	WLAN	x	-	-	-	x	x
[?]	-	-	x	x	-	WLAN, Satellite	x	x	x	x	x	-
[?]	-	x	x	-	-	WLAN	x	-	-	x	x	-
[?]	-	-	-	-	x	-	-	-	x	x	x	x
[?]	-	-	x	-	x	WLAN, WiMAX	-	-	x	x	x	x
[?]	-	-	x	x	x	WLAN, WiMAX	x	-	x	-	x	x

Table II
CLASSIFICATION BASED ON CONVERGENCE AND INTEROPERABILITY

IV. ANALYSIS

Based on the above, the interrelation between WSN and cellular networks is not quite clear at present, although the interrelation between cellular networks and MANET is defined better, probably motivated by the user participation in such networks. Maybe the interaction between MANET and WSN is more feasible, although to this end the MANET devices should be adapted to perform communication with sensor devices (e.g. by modifying the protocol stack). However, the power consumption that a device could need to be connected to a MANET may still be too high for a sensor.

Furthermore, there are some QoS and security requirements to be considered by the network interoperability architectures in the FI. An important key for these schemes to being effective is to avoid the possible attacks that affect to the performance.

A. Quality of Service

In our approach we consider different ways of understanding the QoS. For example, in WSN the QoS must be seen from the viewpoint of the lifetime, and how to extend it to enable the WSN to keep working for as long as possible. Therefore, in the case of WSN it is possible to see the network as a single service, and if we immerse ourselves in it we can probably determine what parameters have to be considered in order to prolong the lifetime as much as possible. Likewise, other types of networks can also have their own requirements and needs to keep their usefulness and continue to provide services. We call these requirements the QoS inherent to the network, or special QoS characteristics of the network.

Moreover, a key point of the the traditional QoS mechanisms for data transmission is the network congestion management. Several studies conclude that the effectiveness of such mechanisms is high in moderately congested networks, but are useless in scenarios with low congestion and unworkable when congestion is high in the system. Therefore, after a threshold (that depends on the system's characteristics) a QoS mechanism can become a burden to the system instead of alleviating it. This type of QoS, more general and dedicated to data transmission, helps to ensure the efficient management of network resources, becoming more useful as the number of participants in the network increases, but also more complex

to implement since it usually requires either reservation of resources or the establishment of priority schemes.

We conclude that each network has its own QoS features that should be prioritized for their subsistence, and further QoS characteristics more general for the communication. In fact, it is possible that the QoS for the communication matches with the QoS specific for an environment, but otherwise will be necessary to find a consensus and to determine the requirements that are of higher priority based on the context, to adequately orchestrate the behaviour of the system. Therefore, the policies in the node should depend on the context at a particular time, and may change dynamically as environmental conditions vary.

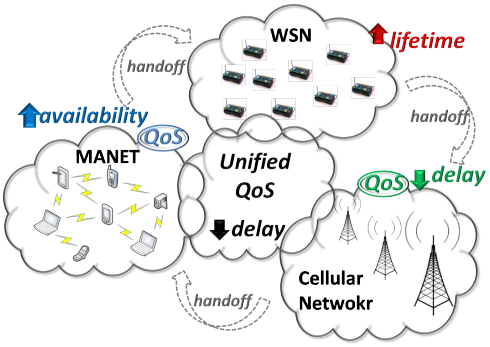

Figure 2. Unified QoS

Figure 2 shows this idea. Each network has its own needs, but share common concerns in the transmission medium used for interoperability. Currently this is possible using border gateways in each network. However, the difference with the new approaches is that for total interoperability among networks, in which an element of any network can connect to a different network, the nodes have to be able to adapt to changing QoS requirements whilst respecting the QoS requirements of the visited network. The main objective should be that the node can enjoy the services that other networks can provide it (e.g. Internet connection, access to environmental information, etc.) but always without interfering negatively in the QoS of the visited system. The big challenge is how to do this while preventing nodes with fewer resources to be seriously damaged during interoperability. Furthermore, the adaptation of some devices could require hardware modifications, and this could be an unappealing option for manufacturers if the return on investment does not compensate them.

B. Security

AAA Services have an important role in cellular networks, but maybe could be extensible to other networks with the aim to seek a unified security architecture. As we have already seen in Section II, cellular networks can provide security to other architectures by using these services. Indeed, while the QoS within each network can have its own characteristics that must be preserved, security usually shows common needs, at least in the three types of networks studied. Therefore, it could be assumed that future security mechanisms tend to be distributed and collaborative. These two features can be difficult to implement if there are different business domains involved. Service providers are cautious about sharing information with each other for several reasons. For example, there is the risk of confidential information leaks from one company to another, that could affect the sale of commercial products. However, maybe the most damaging aspect is that the exchange of information affects to user's data privacy. In such case, it might incur individual or collective demands, coupled with the possible compensation expense. This could damage the reputation of the service provider.

Figure 3 shows a possible security scheme for security cooperation. To avoid the unnecessary redundancy, the security mechanisms must be developed taking into account the open scheme that represents the FI, where the networks become open architectures that promote the cooperation between services. Thus, these mechanisms should be able to adapt to the environment where they are deployed, as well as to provide additional tools for allowing the cooperation between different networks without affecting the QoS. In addition to these local control mechanisms, it is necessary to deploy private (*Pr*) and public (*Pu*) security cooperation architectures to provide the security and trust mechanisms necessary for the exchange of sensitive information. The aim is to allow the authentication of individuals while, at the same time, avoiding the traceability of information that could be analysed by unauthorized entities. *Pr* is the responsible for data exchange between service providers (*SP*) and other entities subject to data protection laws or other requirements. Thus, *Pu* uses the information provided by the users to define models of trust and security mechanisms for enabling the secure cooperation between networks. The final objective is to allow both architectures to coexist and benefit each other.

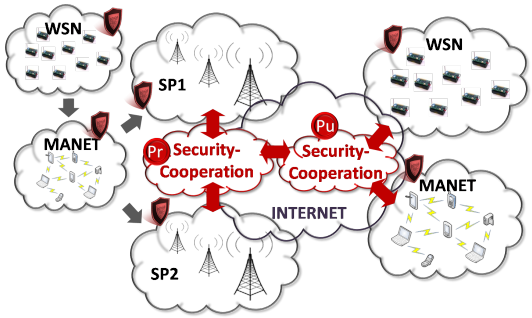

Figure 3. Cooperative Security

The difficulty of this solution lies mainly in the fact that in order to determine whether the information provided is reliable or not (especially in the case of *Pu*) it is necessary to deploy trust mechanisms on a large scale. However, currently there are cooperation mechanisms in social networks or online forums that allow to the users to judge and penalize misbehaviours in the network. The improvement of these techniques and their integration into a common collaborative framework could provide great benefits for security in the FI.

C. Attacks that affect to the performance

The problem of the attacks that affect the performance is that, in the most cases, it is very difficult to accurately predict if the network is under attack or, if instead of that, the network conditions are changing due to other cause, especially in dynamic networks. If both QoS and Security mechanisms can collaborate, then it is not only possible to prevent the corruption of QoS mechanisms, but also to avoid some additional traffic. For example, the QoS mechanisms perform a study based primarily on parameters that indicate the network performance (e.g. throughput, delay, packet loss). This analysis is also of interest for the early detection of attacks, and to detect anomalous behaviour in networks that follow a predictable behaviour. Then, the Intrusion Detection System (IDS) can work with the QoS mechanisms to obtain said information without generating additional traffic. We cannot forget that, while in some environments the additional traffic is not a problem, in resource-constrained networks (e.g. WSN) the repeated transmission of data can be damaging. Moreover, the attacks that affect to the performance are a big problem for network integration, since the effect of such attacks can be propagated through all the collaborative structure producing a very undesirable chain reaction. Indeed, if an attacker affects any of the parameters indicated in Figure 1, then it is relatively easy that this affects the other parameters. However, an advantage of the collaboration between networks is that, if a network that is providing a service has to be isolated, it could be feasible to find another network to replace it in a short period of time. Also here it might be possible the abuse (e.g. an attacker isolates a network to force the use of another network) if the security architecture is not sufficiently robust and the QoS mechanisms of the networks are not able to avoid a total network collapse.

V. Conclusions and Future work

In this paper we have presented an analysis of the current state of technology in network integration, focusing especially on the study of security and QoS issues. In addition, we have proposed high-level integration architectures for those networks in the Future Internet scenario. Based on our research, we conclude that there are important security and QoS problems that must be solved before full integration becomes a reality. Such problems must be solved prior to any integration because a fault in one system could spread through the network. Further steps should be directed to consider the cooperation among networks through Internet and to optimize and secure these communications as far as possible. A key point is the development of efficient security cooperation architectures to take advantage of the massive network interconnection that promotes the Future Internet.

VI. Acknowledgment

This work has been partially supported by the Spanish Ministry of Science and Innovation through the projects SPRINT (TIN2009-09237) and ARES (CSD2007-00004), being the first one also co-funded by FEDER. Additionally, it has been funded by Junta de Andalucia through the project PISCIS (TIC-6334). The first author has been funded by the Spanish FPI Research Programme.