A. Nieto, and J. Lopez, "Analysis and Taxonomy of Security/QoS tradeoff solutions for the Future Internet", *Security and Communication Networks (SCN) Journal*, vol. 7, pp. 2778-2803, 2013.
http://doi.org/10.1002/sec.809
NICS Lab. Publications: https://www.nics.uma.es/publications

Analysis and Taxonomy of Security/QoS tradeoff solutions for the Future Internet

Ana Nieto and Javier Lopez

Computer Science Department, University of Malaga, Spain
Email address:{nieto, jlm}@lcc.uma.es

ABSTRACT

Motivated by the growing convergence of diverse types of networks and the rise of concepts such as Future Internet (FI), in this paper we analyse the coexistence of security mechanisms and Quality of Service (QoS) mechanisms in resource-constrained networks, that are relevant types of networks within the FI environment. More precisely, we analyse the current state of the research on security and QoS in the integration of Wireless Sensor Networks (WSNs), Mobile Ad-Hoc Networks (MANETs) and cellular networks. Furthermore, we propose a taxonomy to identify similarities among these technologies, as well as the requirements for network interconnection. As a result, we define a dependency-based model for the analysis of Security and QoS tradeoff, and also define a high-level integration architecture for networks in the FI setting. The final goal is to provide a critical point of view that allows to assess whether such an integration of networks can be both secure and efficient.

KEYWORDS
Security; QoS; WSN; MANET; cellular networks; IoT

1. INTRODUCTION

Part of the recent research on information technology is focused on convergence and network integration, with the aim of benefiting from features provided by the different types of networks. As a consequence, there is a growing convergence in order to achieve the *all-IP* and *always-on* paradigms. While the first provides the common infrastructure for network communication, the second focus on the need of permanent connection to the Internet. Moreover, the definition of new concepts as Future Internet (FI) or the Internet of Things (IoT) encourages such steps towards the convergence of networks.

The concept of FI is concerned with the future interconnection of heterogeneous networks. For instance, within FI, the IoT considers as an essential requirement the interaction with any object of the real world, where the user will be necessarily and inevitably involved. The ideal scenario is one interconnected world where *things* can connect to each other and users are able to interact with those *things* using the technology deployed for this purpose. From our point of view, one of the main challenges is how to deploy the interoperability mechanisms in that scenario without compromising the security and the quality of service (QoS) in resource-constrained technologies. One key challenge is, for example, how to use the wireless sensor networks (WSN) in an interoperable scenario where the user is involved. In fact, users' dependence on new technologies is fundamental in determining the future networks because society is more likely to keep the technologies that serve a purpose. In that sense, WSNs, mobile ad hoc networks (MANETs) and cellular networks are expected to become key networks within the IoT and the FI due to the advantages that they provide to users.

Wireless sensor networks and other resource-constrained technologies such as radio-frequency identification, make possible the inclusion of the *things* in the IoT. In particular, it has been demonstrated that less-powerful technologies such as radio-frequency identification can communicate with WSNs in a secure way [1]. As a result, WSNs become interesting from the perspective of network convergence because they allow the interoperability with less-powerful *things* and also with less-restricted devices, as we shall see later. Moreover, sensor networks are formed by self-organized devices and the latest technologies add firmware over the air updates, making SW changes more flexible. On the other hand,

cellular networks are intermediary networks* that allow users interaction. User dependence on mobile phones and smartphones have greatly increased, and they are getting closer to offering the same functionality required by a Web/application user, hence evoling from specific-purpose platforms to general-purpose platforms. The way in which users interact with each other (social networks) is transforming the personal devices into MANET in several scenarios, where the ad hoc communication is required. Nonetheless, behind the mobile phones, the infrastructure provided by Service Providers is not resource-constrained. Moreover, security mechanisms are currently applied though within a closed and private environment.

Consequently, WSNs, MANETs and cellular networks are closely interrelated. Although WSNs and MANETs can be part of the IoT, cellular networks are more related to the FI and the role of the user in it. In any case, we understand that the relationship between these three types of networks is very interesting from the point of view of convergence within the IoT. For example, sensors can help with early-detection of changes in environmental conditions where they are deployed (e.g. *things* monitoring). However, energy restrictions means they are less able to transport this data directly through a powerful network without the use of an intermediary. The optimal situation would be for the sensor to be able to communicate data to a device within a MANET, for example, so that it could delegate the transmission of urgent data to a powerful device without draining its own battery. This is not always possible, and is highly dependent on the scenario.

Moreover, and related to user acceptance, ensuring security is a key issue, and generally enhances the user's quality of experience (QoE). In the generic FI scenario, where a wide variety of devices coexist in different domains composed of a myriad of entities, security becomes one of the main issues to be addressed. More precisely, in order to encourage the collaboration of those entities, it is necessary to develop mechanisms for a secure data exchange among them. Yet, 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 systems that are highly secure but non-useful from the point of view of usability. Currently, a security failure or incorrect QoS requirements can affect the correct operation of a network. Once the networks begin to fully interoperate, security and QoS problems will affect the correct behaviour of interconnected networks if necessary precautions are not taken beforehand.

Although both security and QoS mechanisms are essential in the FI, security and QoS are inherently conflicting features. In fact, the issue arises because, while 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 same resources. It is essential to seek a balance between security and QoS in order to build efficient, scalable and secure architectures that are able to make optimal use of resources while maintaining the necessary security level.

*Cellular networks use resource-constrained devices (smartphones) and a infrastructure composed of powerful devices (e.g. long-range base transceiver stations).

1.1. Objectives

The objective of this work is to analyse the current state of security and QoS interdependencies in the integration of resource-constrained networks that are an important part of the FI. We have chosen resource-constrained networks because, despite the analysis of the Security and QoS tradeoff being more complex, efficient protection of the weaker devices is key for the total network convergence. In more detail, in this paper, we focus on security and QoS integration of WSNs, MANETs and cellular networks. These types of networks are excellent candidates for the aforementioned research because of their proximity to the user and overall contribution to society. Thus, we intend to draw conclusions on how close we are to the new FI paradigms becoming a reality in which the user not only feels comfortable but also safe.

1.2. Motivation

Currently, there are several studies that deal with network integration but without explicitly considering the interdependencies of security and QoS requirements as we do here. Also we find in the literature, diverse approaches focusing on the study of Security and QoS tradeoff. However, most of them focus on a specific network architecture, and do not follow general parameters. Our first step is to explore the state of the art in order to find the similarities and differences that make the integration of the technologies discussed in this document difficult.

1.3. Document structure

The paper is structured as follows. In Section 2 we present an overview of the technologies covered in this approach, while in Section 3 the state of the art with respect to security and QoS issues is carried out individually for each type of network. After this, in Section 4, we discuss current efforts to provide interoperability between WSNs, MANETs and cellular networks. The idea is to separate those general characteristics and requirements that are present in all the networks under consideration (*general requirements*) from those that are special/unique characteristics in each one (*inherent to the network*). Given this, in Section 5 we propose a taxonomy of technologies based on QoS and security requirements for the identification of common features and interest between the technologies. For the first result, in Section 6 we propose a parametric model to identify the parametric relationships between security and QoS parameters. This

taxonomy and the model support the analysis carried out in Section 7, where we propose QoS and security schemes for FI network cooperation. Finally, in Section 8 we present our conclusions and future work.

2. THEORETICAL AND PRACTICAL FUNDAMENTALS

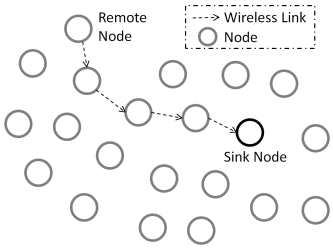
In this section, we present an overview of the resource-constrained networks addressed here. Given the dynamic nature of MANETs and Cellular Networks, the mobility management technologies over internet protocol (IP), mobile IP version 6 (MIPv6), and media independent handover (MIH) are analysed. The first allows roaming between different networks (e.g. wireless local area network (WLAN), worldwide interoperability for microwave work (WiMAX), and universal mobile telecommunications system (UMTS)) without loss of connection [2], while the second allows the handover between different network technologies at low level. Thus, from the viewpoint of network technologies we cover those networks that we believe will play an important role in the Future Internet.

2.1. Resource-constrained networks

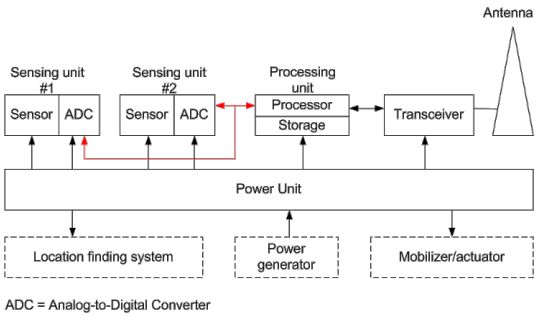
The limitations on physical and logical resources, such as memory or power capabilities, are present in all computers. However, as a natural evolution, there are devices designed to be tiny in order to achieve new functionalities, and this reduction makes resource management in these systems more difficult. The problem is compounded when these devices need to communicate with other devices, because the transmission of data is one of the operations that consume most of the battery, and not all devices have a power supply. In particular, here we examine the integration between WSNs, MANETs and cellular networks. Previous studies such as [3] endorse the study of these networks as particularly significant from a security point of view. Unlike in said paper, in this paper we focus on the Security and QoS tradeoff in the communication between these networks.

2.1.1. Wireless sensor networks.

Wireless sensor networks (Figure 1) are composed of sensors, *autonomous devices* built to solve a specific problem, with limited functional capabilities (only those essential for solving the problem) and resource-constrained (e.g. limited battery). WSNs are used to monitor physical or environmental conditions within an area (e.g. temperature, humidity, radiation, location of animals, etc.). There is a wide variety of sensors, each of them designed to obtain physical measurements from their surroundings (e.g. light, temperature, acceleration/seismic and magnetic measures among others). The popularity of sensors is increasing, precisely because there are many types of sensors, where most of them are autonomous units designed to support tough *environmental conditions* and can be *replaced easily* by other units should any of them stop operating.



(a) Wireless Sensor Network



(b) Architecture of a Sensor [4]

Figure 1. Wireless sensor network.

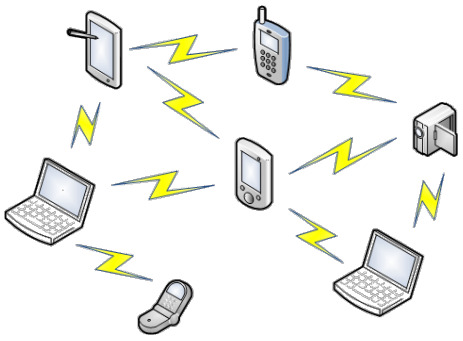


Figure 2. Mobile ad hoc network.

In fact, one of the advantages of sensors is their number. It is to be expected that a sensor network will be composed of a *large number of sensors*, where several of them obtain environmental data in the same area. Then, such measurements are routed to a principal node called Sink that collects all the data from the network. Each node has the capability to *collect and analyse data* prior to sending them to the Sink node [4]. Although it is possible to send the data directly to any of the sensors within the range of the sensor source, the communication between nodes should be *hop-by-hop* in order to save energy [5]. The ideal location for the Sink node is at the centre of the network, because the greater the distance between the source and the Sink, the higher the number of intermediate sensors

to be used to route the information, and more energy is consumed in the process. We have to note that if all the data are routed to the Sink node, then those nodes nearest to the Sink experience a high amount of traffic in contrast with the nodes that are farther from it [6]. For this reason these nodes could use up their energy long before the rest of the nodes in the network. Moreover, it is essential that the Sink node keeps its connectivity with the whole network at all times because, otherwise, the loss of data could render the network useless. Some WSNs define the set of regions of the network that are essential for a good performance (called *area of interest*). In these cases, the Sink has to maintain the connectivity only with those areas to ensure the correct operation of the network.

2.1.2. Mobile ad hoc networks.

Likewise WSNs, MANETs (Figure 2) are composed of *self-configuring* devices connected wirelessly by *multi-hop* communications. However, a WSN should be composed by devices of the same type in order to optimize the resources, while MANET are *dynamic* networks that can be composed of *heterogeneous* devices. Thus, the main motivation for the deployment of a WSN is to obtain information about the environment, and they are generally composed of hundreds of devices that perform similar operations. If a node is damaged or lost, then we can simply replace it with another one. In a MANET, the devices are *close to the user* (e.g. laptop, PDA) and can store *private data*.

Therefore, the devices in a MANET can not be easily replaced, not only because of the cost, but also because they contain user data (e.g. photos, contact address). Indeed, in MANET scenarios there are new security and QoS considerations to be taken into account. While the attacks on WSN can be geared towards falsifying the measurements of the environment, the attacks on MANET can be intended to trick the user or obtain personal data.

Furthermore, the communication architecture for a sensor is cross-layered many times in order to optimize the available resources, while a MANET uses transmission control protocol/IP architecture to allow the interoperability between different devices. The cross-layer architecture enables the common functionalities to be directly accessed from different modules. This approach, that optimizes the access to general functions can be very difficult to manage in complex systems due to the possible existence of dependencies.

2.1.3. Cellular networks.

Cellular networks are composed of cells, where a *cell* is defined as the physical space of coverage of a *base transceiver station* (BTS). The BTS provides wireless coverage to all the mobile devices in its cell. The mobile devices can change cells while they are on the move and still be connected to the network through the BTS of the new cell. In contrast to the WSN, the cellular networks are dependent on *service providers* and need a *network*

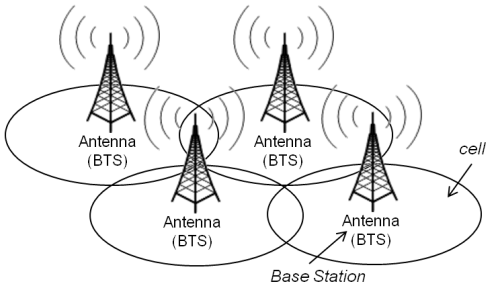
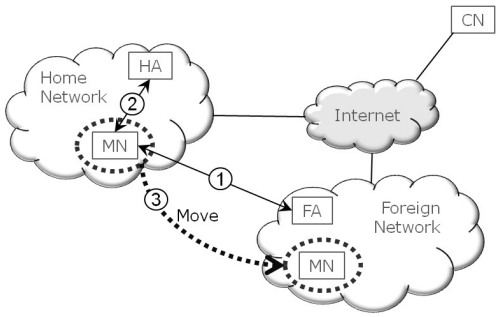
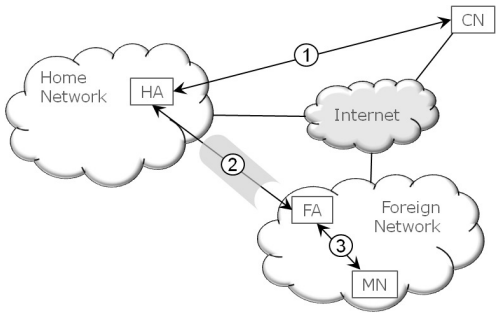


Figure 3. Cellular network.



(a) Networks before mobility



(b) Networks after mobility

Figure 4. Mobile internet protocol.

infrastructure to allow authentication, authorization and accounting services (AAA Services). The *AAA Services* help to control the use of the network by the user for subsequent *payment*. It is worth mentioning here global system for mobile communications (GSM), UMTS and long term evolution (LTE), as each one of them represent the beginnings of a new generation in cellular networks.

Specifically, the first notions of security appeared with the GSM specification. Here the security mechanisms can be divided into two types: the first used for communication security and the second to protect the terminal against unauthorized use. The first in GMS are: the subscriber identity module (SIM) card, the international mobile subscriber identity (IMSI) that is unique to each user, a secret key and cryptographic algorithms. In order to protect the unauthorized use of the terminal the international

mobile equipment identity (IMEI) was defined, a *unique identifier per terminal*. The IMEI can be used to remotely disable the terminal in case of theft or loss. The IMEI is written into the hardware of the mobile phone, and the device can only be disabled by a service operator.

Moreover, the UMTS specification introduces packet switching and therefore security and QoS improvements, as for example the use of public key cryptography or increased bandwidth. Over the years, mobile terminals have been increasing in complexity, not only as a measure of protection, but also looking to increase *user satisfaction*, for example promoting the use of new services and *improving the connectivity of terminals to other networks* (e.g. Internet) or devices (e.g. Bluetooth). The fourth generation of mobile terminals (4G) is expected to be based on *all-IP* based technologies. Moreover, the network will offer higher bandwidth and support for different access technologies (e.g. IEEE 802.11) and multimedia applications [7]. UMTS Long Term Evolution (LTE) is a 4G technology optimized for packet switching, with a simplified architecture that enables faster data transfer at low cost and energy [8].

2.2. Internet protocol mobility management protocols

Mobile IP (MIP) is a standard communication protocol designed to enable mobile users to move from one network to another while maintaining a fixed IP address [9]. MIP allows *macromobility*, namely the change from a network (home) to another (foreign), transparent to other users (Figure 4). *Transparency* is possible because the IP datagrams are forwarded from the home network to the foreign network. However, the *redirection* of traffic and the migration of the node affect the performance of the network.

On the one hand, MIP uses *intermediary entities* that know the current location of the node for traffic redirection. This can increase the *overhead* in both networks, home and foreign. On the other hand, during the migration process (known as *handoff or handover*) some packages addressed to the mobile node can be lost. The performance problem is compounded if we also consider the security of the network, because in that case it may be necessary to establish *AAA Services*.

Generally, such controls are established before the network change is effective and can involve multiple participants. The *handover* process is critical to network performance. If this process drags on, then the connection may be interrupted. Moreover, the user may perceive a poor connection, even detect the change of network, affecting the transparency. Besides, reserving network resources before data transmission creates several problems [7]. Indeed, the resource reservation process (QoS signaling) implies a waste of network resources itself (e.g. bandwidth for network communication).

The consumption of resources when performing *QoS signaling* is compensated because posterior communications have the *availability* of such resources guaranteed for data transmission. However, in mobility scenarios applying QoS Signaling techniques may not be justified because successive changes in the network may involve the new calculation of new routes for the delivery of data. Thus, the network resources can be consumed in maintaining the resource reservation indefinitely.

In addition, the *media independent handover* (MIH) technology, published in 2008 (IEEE 802.21 standard), allows the handover among different network technologies (*vertical handover*). The MIH protocol provides low-level mechanisms required for the improvement of the performance of MIP. One of the motivations of MIH is to enable a *common information service* to provide a global network map with data about the available networks within a location (e.g. a cellular network may indicate the presence of a suitable WiFi station). This information service would be managed by the operators, and users could have access to the information via their mobile devices. MIH defines its own messages to the MAC layer. For example, a client with MIH could change the connection from WiMAX to 3G WWAN, *without loss of connection* [10].

2.3. Internet protocol security protocol

The IP security protocol (IPsec) can be added to any of the current versions of IP (IPv4 or IPv6) using additional headers to provide: *authentication*, *confidentiality* and *key management* [11].

IPsec does not implement non-repudation, protection against DoS attacks or traffic analysis. IPsec uses the *Authentication Header* (AH) and the *Encapsulating Security Payloa*d (ESP) protocols. The first one is an authentication protocol, while the second one combines encryption and authentication. The ESP and AH protocols enable IPsec to create secure tunnels for communication, the *Virtual Private Networks* (VPN). Specifically, IPsec defines two ways of packaging: transport and tunnel.

On the one hand, in the *transport mode*, the respective headers are located after the headers that have to be read by the routers (IPv6 head and optional headers) and before the payload (cyphered data that should not be read until it reaches its destination). On the other hand, in the *tunnel mode*, the entire original IP datagram is encrypted and placed as data. Then, a new IPv6 header is created with the basic data to carry the packet to its destination. This mode allows the full authentication of the IP datagram, while the transport mode only authenticates the payload.

From a *performance* point of view, the transport mode requires less time to complete the data packaging and the final datagram is smaller. In many cases authentication of the whole datagram does not have a significant advantage. For example, if probability of attacks is low, then the transport mode can be a better option than the tunnel mode.

3. SECURITY AND QUALITY OF SERVICE TRADEOFF IN WIRELESS SENSOR NETWORKS, MOBILE AD HOC NETWORKS AND CELLULAR NETWORKS

Prior to considering network integration, it is necessary to identify the specific characteristics that are of importance for each network individually. In conjunction with the study carried out in Section 4, it is possible to identify those parameters that are important in both a specific network and in a collaborative environment (general parameters), and those that are mainly relevant in a specific network environment (specific requirements, or inherent to the network).

3.1. Wireless sensor networks

3.1.1. Deploying security mechanisms in wireless sensor networks.

Studying the impact that security mechanisms have on QoS in the scope of WSNs becomes a challenging task [12]. Moreover, deploying security features in sensors that are connected directly to the Internet can be a daunting task [13], and traditional security mechanisms are not always suitable for use in WSNs [14, 15]. 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 [16]. In particular, *routing tasks* consume more energy [17]. 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 [18].

Routing protocols must consider not only the node closest to the destination or the safest node (although this may depend on the context), but also their energy levels [17]. Moreover, security mechanisms may cause overhead. For example location privacy in sensor networks may require packet injection increasing transmission and therefore increasing energy consumption [14].

3.1.2. Security as a key factor for performance in wireless sensor networks.

Paradoxically, the lack of security mechanisms can have negative consequences for QoS in WSNs. Thus, in [19], the effect of not providing the properties of confidentiality, integrity, authenticity and availability in a sensor network is studied. The study encompasses various WSN technologies, namely wireless interface to sensors (WISA), WirelessHart, ISA 100.11a, ZigBee and 802.15.4 medium access control (MAC). The results of this work show 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*. In addition, the study shows that the standards are still vulnerable to jamming, collision and flooding attacks, which affect the QoS of the system, and also that the QoS and security support for heterogeneous network segments remain unexplored fields.

While the approach in [19] shows that security can prevent QoS degradation, [20] states that QoS is a requirement for security in a sensor network. In that approach the security levels are classified based on the confidentiality of information, data integrity and availability of resources. The QoS is discussed in terms of availability, reliability and serviceability, also taking the energy performance into account. Indeed the *availability* can be considered as a security requirement [21], and is a key factor for good *intrusion detection*. For example, the availability of the devices within an intrusion detection system (IDS) or the databases that store the evidence of attacks are critical factors to be considered.

3.1.3. Data redundancy and hierarchy.

Another aspect to consider is data redundancy. In WSNs, several sensors can cover the same area, and therefore they can produce the same event. This redundancy allows the sink node to assess whether the event is valid or, whether it is in fact an anomaly. For example, in a forest in which sensors are deployed for fire detection, if all the sensors in an area except one detects the presence of fire, it probably means that the sensor that did not detect the event is wrong. Similarly, if only one sensor warns of a fire and the rest of the sensors indicate otherwise, then it would be more probable that there is no fire.

The relationship between *data redundancy, reliability, energy consumption, data fusion and network delays* is studied in [22]. In fact, *the more data redundancy, the more reliable the information is*, although the sensors use more energy in delivering data.

In order to *alleviate the energy consumption* due to data redundancy, *data fusion* proposes that the data is summarized before reaching the destination node. For example, if there is a hierarchical structure, the cluster head could decide whether there is a fire and lead the response to the sink node or the next cluster head in the hierarchy. However, this process of fusion may cause *delays in the network due to the decision process*, and the cluster heads must devote part of their resources to that end.

Regarding security, the fusion process is very appealing to an attacker, it does not have to misrepresent or impersonate any nodes but must discover the cluster heads and replace them. Therefore, the clusters not only become potential bottlenecks, they become key points for distortion of the measurements of a WSN environment.

3.1.4. Deploying quality of service mechanisms in wireless sensor networks.

We cannot forget that even ensuring QoS (without considering the security requirements) would not be trivial in these systems, because in order to offer QoS guarantees, we need a certain degree of *predictability*, difficult to provide for the vast majority of resource-constrained networks or dynamic networks due to, for example, changes in network topology [23, 24].

The predictability is related to *resource reservation*, which is a common technique in QoS mechanisms. The protocols for resource reservation guarantee that a path is available for transmission within a period of time. To do this, these protocols require the sending of requests to reserve resources through various paths in the network, thereby consuming the resources available for data transmission. Additionally, the use of such mechanisms leaves the network exposed to QoS signaling attacks, in which an attacker reserves unused resources. The result is that, on the one hand, the legitimate nodes can not reserve resources for their own use (*denial of service (DoS)*), and on the other hand, the intermediary nodes waste their energy in the *QoS signaling* process.

If the *network topology* is known, the attack could be targeted at specific nodes (eg. cluster nodes) to damage the network connectivity. In the case of the WSN we also have to take into account the *environmental conditions* that can affect some devices in the network. 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 [25]. So, for intrusion detection it is necessary to consider these conditions, and it is not always possible to distinguish beyond any doubt, and in real time, whether the network is under attack or if it is experiencing failures due to other external factors.

3.1.5. Summary.

To conclude, implementing security or QoS mechanisms in sensor networks is not trivial, even less so when we intend to implement both mechanisms simultaneously. The nodes are resource-constrained and, thus, from a performance point of view, these mechanisms are very costly to implement. The QoS mechanisms for sensor networks are simplified, generally focusing on extending the network's lifetime. The vast majority of efforts to adapt QoS traditional techniques to sensor environments are intended for the wireless multimedia sensor networks (WMSN) [26]. However, if security and QoS mechanisms can be properly integrated into WSNs, this could provide advantages from a security and performance point of view if both types of mechanisms can collaborate with each other. There is a key point here, that is the additional dificulty of distinguishing a real attack from a change in the network due to environmental conditions, or changes in the network topology (e.g. due to mobility).

3.2. Mobile ad hoc networks

3.2.1. Deploying quality of service and security mechanisms in mobile ad hoc networks.

Generally, 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 Integrated and Differentiated Service protocols (IntServ and DiffServ) [27].

For example, in [28] the authors analyse the security threats in resource reservation (QoS signaling) in MANET, using the INSIGNIA and SWAN protocols, respectively, based on IntServ and DiffServ. In this case, while INSIGNIA ensures sufficient resources along the communication path, SWAN makes an estimation of available resources along the path. The paper concludes that, regardless of the protocol, one problem 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 paper [29] lists several security and QoS problems in MANET, but focuses on intrusion detection mechanisms to detect and prevent QoS signaling attacks.

Thus, in [30] the authors focus on defining the DoS-resistant QoS (DRQoS) protocol, a QoS signaling protocol for MANET resistant against some variants of flooding and over-reservation attacks. In order to do this, each node needs to store an entry in a state table for each stream of communication that attempts to transmit. This means that a node has an entry *(i, j)* for each neighbour node *i* and *j* that communicate through it. Managing these tables can be somewhat complex and costly given the dynamic nature of MANET.

3.2.2. Self-organization and dynamic nature.

Furthermore, a particularly interesting feature of MANETs is their capability 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, in [31] the author defines 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*. Specifically, Chamaleon (CML) is proposed as an adaptive routing protocol for MANET.

The use of IPsec in MANET was studied in [27], the paper shows that at MAC level the frames would be protected using the IEEE 802.11i protocol, which adds protection hop-by-hop. In order to do this, the

encryption is performed hop-by-hop, so it may requirs the intermediate nodes to have *pre-shared keys* or to be enabled to use *certificates*. The proposed solution is for a military scenario, where the pre-shared key assumption is a feasible option (uses a symmetric key) and only considers one QoS domain, so the problem is simplified. The IPsec AH header is modified to include the values data services (DS) and explicit congestion notification (ECN) as well as an optional field that can be used by attackers, verifying the integrity of these data by the integrity check value (ICV).

3.2.3. Summary.

Based on the above, there are current approaches for adapting traditional QoS mechanisms (DiffServ, IntServ) to MANET, in order to perform the resource reservation and its maintenance (QoS signaling). However, QoS signaling protection is fundamental to avoid DoS or similar attacks that have a negative impact on the resource availability in MANET. Nevertheless, the dynamism in MANET makes the intrusion detection difficult, which should take into account the input and output of nodes in the network, as well as their mobility within it.

3.3. Cellular networks

3.3.1. Business considerations.

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. In [32] the importance of dealing with attacks that affect the performance and availability of cellular networks is studied. In particular, theft-of-service (ToS), Denial of Service (DoS) and IP spoofing attacks. In fact, these attacks can damage the service provider's reputation and this may incur 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. So, in [33] the combined use of *elliptic curve cryptography* (ECC) and symmetric key to address the vulnerabilities of a 3G-WLAN hybrid system is proposed. ECC is more *energy efficient* than private key cryptography, and with a shorter key length can result in a level of *safety* equivalent to that provided by public key cryptography.

3.3.2. Internet protocol-based mobility in cellular networks.

The IP-based mobility is also a hot topic in this area. For example, in [7] the architecture SeaSoS is proposed. SeaSoS integrates QoS Signaling, AAA Services 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. The paper shows a comparative table with the security, QoS and mobility mechanisms used in other studies based on 4G architectures. From this comparison it is noteworthy that most of the mobility protocols used in the solutions are based on MIP, with the exception of W-SKE protocol [34], which focuses on *efficient key management* (creating, distributing, etc.).

Along the same lines, in [35] Tiny SESAME is proposed. Tiny SESAME is a security mechanism based on the SESAME architecture for distributed systems that extends Kerberos with additional security mechanisms. Tiny SESAME [35] 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. As a restriction, the mobile client should be able to run Java code, which is too aggressive for resource-constrained devices, so an open challenge in such work is to migrate the actual scheme to J2ME (Java 2 Micro Edition), a more lightweight language for software development.

3.3.3. Behaviour-based context.

Moreover, in [36] the need to provide QoS techniques adaptable to user needs and the importance of developing secure and efficient IP-based services is highlighted. To this end they propose the use of *cognitive techniques* to provide intuitive responses to the changing environment, offering the possibility of selecting a set of parameters appropriate to the context of the device. For example, while the user is on the move the system could obtain information about their neighbours' devices and report the optimal settings (performance and security) based on the *availability* of computer resources. For performance metrics the authors take into account the *distance*, the number of *hops* to destination, the *bit error rate* (BER), the packet *delivery rate* (PDR), the *signal strength*, the *energy*, the *time response*, the *prioritization* of messages and the *call dropping probability* (CDP). This last parameter is specific to 4G networks. These techniques in conjunction with techniques such as keystroke-based authentication [37] help to provide a better service to the user.

3.3.4. Summary.

The coexistence of QoS and security mechanisms in 4G architectures is therefore acceptable, as well as schemes to provide the user with mobility without loss of connection. The ideal scenario is one that will allow these technologies to responsibly coexist with each other in order to seek maximum performance and network efficiency. In addition, these mechanisms will continue to be refined to make them resistant to new threats due to IP-based architecture of the new generations of mobile telephony, without forgetting that the end user plays an important role in the adoption of these new technologies.

4. REQUIREMENTS FOR NETWORK CONVERGENCE AND INTEROPERABILITY

In contrast with the previous section, where individual characteristics were identified, in what follows the aim is to identify the *general parameters and requirements* that have to be considered for network convergence. So, it is possible to determine the impact that a possible collaboration with other networks has on a particular network environment.

This section has been broken down into five subsections in accordance with the current literature, each one dealing with a topic. These topics can be considered to increase the probability of the new interoperability schemes being accepted. Note that, we have also considered the study of Security and QoS tradeoff in IP networks to be particularly interesting, because they can be considered as the core-technology for the collaboration between multiple paradigms (all-IP).

4.1. Providing access to the internet

The future of cellular networks relies on their integration with IP networks [7]. Indeed, several studies consider the use of MIP for 4G mobility management, or all-IP networks in general [38]. For example, in [39] the authors reflect on the problems that may arise in the integration between cellular networks and WLANs, choosing MIP as the mobility protocol. Taking into account this 4G-MIP integration, it is not surprising that in other publications such as [40] the coexistence of *MANET and cellular networks* is proposed. This alliance provides both *security* and *flexibility* advantages. On the one hand, cellular networks can handle *global information* that is very useful for security mechanisms; for example, to authenticate the user or his terminal, or to perform accounting and billing tasks. On the other hand, MANETs lack organizational structure and are highly *dynamic*, so they are currently much more flexible than cellular networks. The approach followed in [40] enables the MANET devices to connect to a cellular network, taking a step towards the cooperation between heterogeneous networks and convergence.

Moreover, in [31] a three level communication architecture is proposed. On the lowest level there is eMANET (emergency MANET), on the intermediate level semi-mobile nodes, and on the highest level a gateway to access an IP Cloud. The proposed scheme targets *emergency rescue situations*. This gives us another perspective of the network convergence and the importance of *self-configuring* and *self-organized* networks such as MANET. Furthermore, the inclusion of communication networks to take measurements of the affected environment, such as *WSN*, can help to prevent the rescue services taking unnecessary risks; for example, warning of high levels of gas, or if there is risk of nuclear leaks (in the case of a nuclear power plant). The integration of *cellular networks and WSN* is proposed in [41], where the 4G paradigm is presented as a combination of heterogeneous networks where the sensors are included. In this sense, the sensors make their contribution to industries (eg. nuclear plants) or at home, and would use *cellular terminals as gateways* for the access to IP networks.

4.2. Always-on as a need

Network integration brings benefits beyond collaboration between networks for exchanging information of interest or the use of services such as providing access to the Internet. In fact, giving the user the possibility to *always be connected to the Internet* (always-on) is very interesting because it favours *business opportunities* for service providers.

Along the same lines, in [42] an architecture to integrate heterogeneous wireless systems used to provide ubiquitous high-speed services to mobile users is proposed. Among the technologies covered are WLANs, UMTS and satellite networks, and IP is used as the protocol for the interconnection. The security is implemented through specific algorithms for authentication and billing, and MIP is used to facilitate the roaming between different wireless systems. Both security and mobility would be managed by a third party, and each operator needs to establish a *service level agreement* (SLA) with it. The idea behind this approach is that the user device connects to the network available with the capabilities to provide the best service for data transmission. For example, assuming that the user's device supports various forms of connection (WiFi, 3G, satellite), if the user is in a WiFi-enabled shopping center, then the device can use the WiFi access point of the commercial centre for access to Internet. However, if that access is not available, then the device could try to use 3G to connect, and finally the device could even use a satellite link, although this last option consumes far more resources than the previous two.

Another approach that seeks to exploit the expected host of alternatives for connectivity is that proposed in [43]. In particular, the study addresses the integration of cellular networks (eg. 1G, 2G, 2.5G, 3G, IEEE 802.20), WLANs (ej.IEEE 802.11a/b/g, HiperLAN/2), WPANs (ej.Bluetooth, 802.15.1/3/4) and WMANs (ej.802.16). It also takes into account the existence of MANET, that can act as routers by using the WLAN/WPAN interfaces[†], and the *AAA services* to provide security. The elements responsible for managing the *load balancing* and *handover* are the *base transceiver stations* (BTS) and *access points* (AP). The drawback is that the *protocol stack* must be modified to include an interface for each piece of technology involved in the MN (eg. cellular networks and 802.11 require different MAC, link and physical levels).

[†] While MANETs are multi-hop networks, other networks listed are single-hop, which means that the nodes send data directly to a specific access point.

4.3. Performance

Furthermore, the *heterogeneity* of devices sharing the same environment can affect network performance by increasing the risk of *collisions*. Nevertheless, *multi-hop* communications can help to reduce the risk of collisions while saving *energy* because the transmission range is less than if directly connected to the BTS or the AP, and therefore requires less power consumption. Furthermore, the collision risk is reduced because the transmission signal does not affect the whole network at the same time; rather, it will propagate from one node to the next node in the path. So, the multi-hop communication allows the effect of the communication signal from the entire network to some regions of the network to be minimised at a given time. However, each node in the path has to use part of its energy in data transmission. For this reason, several studies concentrate their effort on estimating the optimal number of hops in a communication [43].

Please, note that *performance is not the same that QoS*. A clear example of this is that QoS Signaling mechanisms cannot be deployed in all network systems precisely due to the additional traffic that this requires (see Section 2.2). However they are closely related, because improving the performance increases the probability that the system offers a better QoS. Moreover, the QoS can be greatly compromised if the performance is poor. Security mechanisms can also affect performance, because they add network traffic that may cause overhead. So, the security system can interpret the poor connectivity as an attempt against the safety of the network (e.g. denial of service) and perform actions to avoid it (incorrect actions in this case, because it is a false positive).

In conclusion, deploying QoS and security mechanisms can negatively affect the performance, and therefore also themselves. If security mechanisms are able to collaborate with QoS mechanisms and these can be adapted to enhance the performance, then this may help the convergence, reduce the false positives due to changes in the network behaviour and enable the QoS mechanisms to be *scalable* and used in resource-constrained networks.

4.4. Mobile platforms

As we have seen, several studies consider MIP an ideal mobility management protocol for the network convergence, although as has been previously described, MIH is more generic and defines frames designed to manage mobility to MAC level. In this sense, [44] highlight the importance of the *reliability* of the source from which the information is obtained in MIH networks, the need for a *secure channel* between the user and the end point, and the *handover* optimization, especially when handover is performed through *different administrative domains*. In [45] a tutorial on security in MIH networks, indicates that due to the large number of different *AAA domains*, a *pre-authentication* solution in these domains is required. In [44] such a proposal is adopted, as well as the *pre-configuration* of the terminals.

MIH is also used in [46], where the integration of WLANs IEEE 802.11 and WMANs IEEE 802.16 (WiMAX) is analysed. The paper focuses on managing the handover process, where they state that the handover decisions should be based on several factors, among them, the QoS and security support. Moreover, in [47] MIH is used in the handover process between WiFi and WiMAX. The authors recommend that the nodes running critical operations (eg. security decisions that influence the handover process) have to form part of the *core of the network* to decouple to the APs and BTSs of such management. This decoupling is natural and understandable even for heterogeneous networks. For example, in order to include security properties such as the *authentication* of the terminal, the system has to be able to support *efficient and secure data management* (eg. the IMEI and IMSI in cellular networks), but if the communication architecture is distributed with different administrative domains, such tasks can be too complex for the BTSs and APs.

In fact, in order to properly identify users or their terminals, the system has to store *unique identifiers*, and in the case of loss, theft or terminal extinction the system should disable the utilization of these data to avoid fraudulent use by unauthorized parties. Moreover, in distributed systems, the management is more complicated as well as expensive. Taking into account that the user can be directly harmed by system failures or *personal data leaks*, such problems can degenerate into monetary losses for the service providers, owners or coordination managers of the infrastructure and physical media. Therefore, assigning data management to the most powerful and robust services is not a bad approach, but always bearing in mind that this information could eventually pass through the BTSs or the APs, and that intruders have different ways of obtaining information, such as *traffic analysis*, or deliberate damage by performing attacks that affect the performance or availability of services, such as DoS or ToS attacks.

4.5. IP Networks

4.5.1. Security and quality of service in internet protocol.

The most widespread mechanisms for providing QoS guarantees in IP networks are *DiffServ* and *IntServ*, while IP security is provided by the IP security protocol (IPsec).

A very important aspect is the adaptability of QoS mechanisms to *environmental changes*. For example, [48] defines QoS policies that are automatically included in the configuration of network devices, with the possibility of being adapted as network conditions change. The QoS is provided by using the DiffServ provisioning technology, which incorporates mechanisms for classifying, managing network traffic and providing QoS guarantees over IP networks. Tools of such architecture are used to provide

QoS in GESEQ [49], a generic model of security and QoS which uses IPsec to enable secure communications by the deployment of Virtual Private Networks (VPNs).

IPsec is needed in IP networks because IP does not provide data protection over public networks like the Internet. IPsec integrates security features such as source authentication, data integrity, confidentiality, non-repudiation and avoids packet replay attacks by using the sliding window mechanism, although it affects the performance. The QoS mechanisms used in GESEQ helped to improve the performance, quantified according to the *latency*, *jitter* (delay variation) and *packet loss* parameters.

4.5.2. Internet protocol security protocol and quality of service.

Some problems with using IPsec are discussed in [27]. For example, the QoS options are listed in the header of IP datagrams without being encrypted, and therefore are exposed to being interpreted by an attacker. Moreover, in case the QoS options have been encrypted, the intermediate nodes cannot use them without *preprocessing for decoding*. For example, the Differentiated Services (DiffServ) and DiffServ Code Point (DSCP) fields are present in the IPv4 and IPv6 headers to indicate the behaviour of the intermediary routers (hop-by-hop options).

Other options related to QoS, such as the *bandwidth reservation* and *flow differentiation* (not classes, but using a unique flow identifier), are specified by optional IPv6 headers. If the whole package is encrypted, then these options can be useless unless the routers integrate the required functionality to decrypt and encrypt the package (eg. using a preshared key or authorization certificates), but in any case it introduces *communication delays*, even more so when the optional headers are used.

Another drawback is that some protocols require *flow identification* (eg. IntServ) and therefore keep the source and destination IP addresses, port numbers and the protocol identifier visible. This implies that these data could be captured by any sniffer or traffic analyser in the network. There is also the disadvantage of datagrams received out of order, which IPsec tries to compensate for by using different *Security Associations (SA)* for different classes of traffic.

4.5.3. Mobile internet protocol challenges.

Regarding the MIP, current efforts primarily focus on reducing the *handover time* and solving those problems caused by the use of more than one domain (eg. change of domain). For example, the secure, QoS-enabled mobility (SeQoMo) architecture has been developed to provide security and QoS support in MIPv6 [50]. The idea behind this architecture is to mitigate the high *latency* and *overhead* during the handover, while the network infrastructure is protected by security mechanisms such as *authentication* or *authorization* in conjunction with QoS processes. Indeed, the *security in MIP* is provided by additional protocols, like for example the aforementioned *IPsec* or *AAA services*. There are several approaches that consider MIP as a part of the infrastructure for the interoperability in which security and QoS are key requirements. These papers are discussed in the following section.

4.6. Summary

We find that the current approaches are based on tree network architectures, where the mobile nodes are the leaves and the root is an element acting as the gateway for internetwork communication. But it is better to move towards more distributed and dynamic architectures in order to allow any device to connect to the Internet by itself. However, we must solve several difficulties, and maybe the most important is the coexistence and cooperation of services that belong to *different domains*. In other words, currently, it is feasible that different domains use different mechanisms (protocols and policies) to provide QoS and Security, and the problem is that they are not necessarily interoperable.

Moreover, in a heterogeneous environment, *constrained-resource nodes* can coexist with more powerful nodes that could launch an attack that a constrained-resource node is unable to avoid because of its limited capabilities. Another problem is the *cost of deploying distributed trust schemes* or other security mechanisms that require access to *user's data* or the mass storage of information in order to be effective. Furthermore, improving the *handover efficiency* (both horizontal and vertical) is crucial for the integration of heterogeneous networks, as well as enhancing the security mechanisms to protect the infrastructure and its users without negatively impacting on the performance of the handover procedure. However, despite their relevance, both aspects are open challenges. Finally, we have to remember that due to the cooperation among service providers, it is fundamental to take precautions to avoid *unfair competition*. Furthermore, the traceability of information and possible data leaks are aspects to be carefully taken into consideration in environments where user data are handled.

Finally, Figure 5 shows the main topics that have been considered in this paper up to this point, the relationships between them and the main challenges taken from the previous study.

5. ANALYSIS OF EXISTING SOLUTIONS

In this section we define a taxonomy based on previous related work on Security and QoS tradeoff. The aim is to provide an analysis based on current research tendencies and network requirements detected in the previous sections. The taxonomy describes the classification of several papers from the Security and QoS tradeoff point

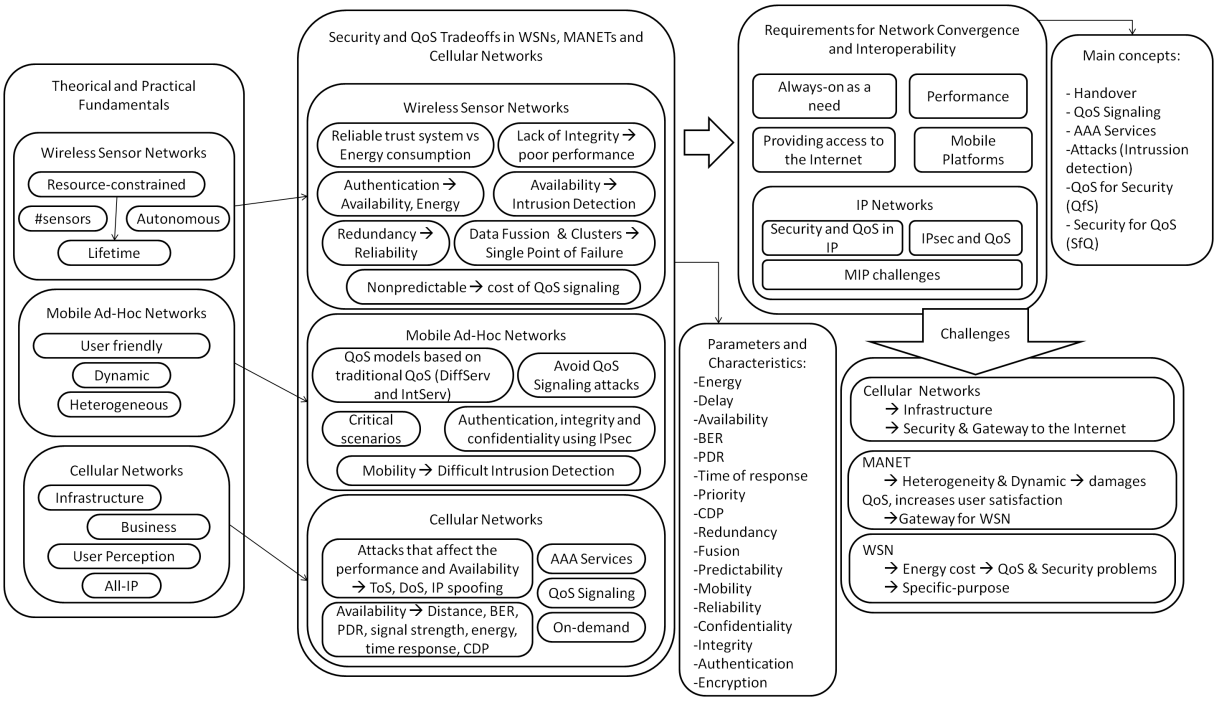


Figure 5. Requirements and Main Topics

Table I. Classification based on features.

	Security								QoS									Purpose		
Paper	Authentication	Authorization	Integrity	Trust	Encryption	Key	AAA S.	IPsec	Delay	Throughput	Jitter	Bandwidth	Packet Loss	Overhead	Energy	Availability	QoS S.	Attacks	P. Analysis	Type
[12]	-	-	-	-	x	x	-	-	-	-	-	-	-	x	x	-	-	-	-	
[13]	x	x	x	-	x	-	-	-	-	-	-	-	-	-	x	x	-	x	-	
[16]	-	-	-	-	-	-	-	-	x	x	x	x	x	-	x	x	-	-	x	WSN
[17]	x	-	x	x	x	-	-	-	-	x	-	-	x	x	x	-	-	x	-	
[19]	x	-	x	x	x	-	-	-	x	x	x	-	x	x	x	x	-	-	x	
[20]	x	-	x	-	-	x	-	-	x	x	-	x	-	x	x	x	-	x	x	
[28]	x	-	x	x	-	-	-	-	x	-	x	x	-	x	-	x	x	x	-	
[29]	x	x	x	x	x	x	-	-	x	x	x	x	x	x	x	x	x	x	x	MANET
[30]	x	-	x	-	-	-	-	-	x	-	-	-	-	-	-	x	x	x	-	
[31]	x	-	x	x	x	-	-	x	x	-	-	x	-	x	-	x	-	x	-	
[27]	x	-	x	-	-	-	-	x	x	x	x	x	-	-	-	-	-	x	-	
[7]	x	x	x	x	x	x	x	-	x	-	-	-	-	-	-	-	x	-	-	
[33]	x	-	x	-	x	-	x	-	x	x	-	-	x	x	-	-	-	x	-	
[36]	x	x	x	-	-	-	-	-	x	x	-	x	-	-	x	x	-	x	-	Cellular
[35]	x	x	x	x	x	x	-	-	x	-	-	x	-	-	-	-	-	-	-	
[32]	x	x	x	-	x	x	x	-	-	-	-	x	-	-	-	x	-	-	-	

AAA S., authentication, authorization, and accounting services; QoS, quality of service.

of view, in order to identify commonalities and differences based on the technology. Moreover, this taxonomy offers a scheme of parametric relationships between Security and QoS parameters identified throughout the study. Thus, we have approached the study from three points of view. Firstly, the characteristics of each type of network are studied in order to find similarities between them (Table I). Secondly, we have studied the requirements for network interconnection (Table II). Thirdly, we also consider general studies related with Security and QoS tradeoff (Table III).

Table II. Classification based on convergence and interoperability.

	Technologies							Type					
Paper	WSN	MANET	Cellular	MIP	MIH	WLAN	WiMAX	Integration	Attacks	QoS S.	AAA S.	Handover	Analysis
[7]	-	-	x	x	-	-	-	x	-	x	x	-	-
[39]	-	-	x	x	-	x	-	x	-	-	x	x	-
[40]	-	x	x	-	-	-	-	x	x	x	x	-	-
[41]	x	x	x	-	-	x	-	x	-	-	-	x	x
[42]	-	-	x	x	-	x	-	x	x	x	x	x	-
[43]	-	x	x	-	-	x	-	x	-	-	x	x	-
[44]	-	-	-	-	x	-	-	-	-	x	x	x	x
[45]	-	-	x	-	x	x	x	-	-	x	x	x	x
[46]	-	-	x	x	x	x	x	x	-	x	-	x	x

AAA S., authentication, authorization, and accounting services; QoS, quality of service; WSN, wireless sensor networks; MANET, mobile ad hoc networks; MIP, mobile internet protocol; MIH, media independent handover; WLAN, wireless local area network; WiMAX, worldwide interoperability for microwave access.

Table III. Classification based on general purposes.

	Security						QoS								Purpose	
Paper	Authentication	Authorization	Integrity	Trust	Encryption	Key	Delay	Throughput	Jitter	Bandwidth	Packet Loss	Overhead	Energy	Availability	Attacks	P.Analysis
[51]	-	-	-	-	-	x	x	-	-	x	-	-	-	-	x	x
[52]	x	x	x	-	x	x	x	-	-	x	-	-	-	-	-	-
[53]	-	-	-	-	-	-	x	x	x	-	x	x	x	-	x	x
[54]	x	-	-	-	-	x	x	-	-	-	-	-	-	-	-	x
[55]	-	-	-	-	x	x	x	-	-	-	x	-	x	-	-	x
[56]	-	-	-	-	x	x	x	x	-	-	-	x	-	-	x	x
[57]	-	-	-	-	x	-	-	-	-	-	-	-	x	-	-	x
[58]	x	-	x	-	x	-	x	x	-	-	x	x	-	-	-	x
[59]	-	x	x	x	x	-	x	x	-	-	-	x	-	-	-	-
[60]	x	-	x	-	x	x	x	-	-	-	-	x	x	-	-	-

QoS, quality of service.

5.1. Classification based on features

Table I shows that, in the research work under consideration, the *authentication and communication integrity* are two properties repeated in most of the research that addresses security issues. This is especially true 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 (*AAA S.*) as can be best distinguished in Table II .

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 for calculating the network *lifetime*. In the particular case of throughput in WSN, it is noteworthy that, although it is a parameter mentioned in several papers, it is not discussed as thoroughly as delay and energy consumption. We must also note that QoS signaling is analysed in several articles related to MANET, where the analysis of *DoS* attacks also has an important role.

5.2. Classification based on convergence and interoperability

Table II analyses the research related with network integration. From this it follows that most of the work considered includes *AAA Services*, the performance and security problems due to *handover*, and *QoS signaling (*QoS S.*)*. Therefore, these approaches reflect the importance of deploying *resource reservation* and security mechanisms and ensuring that such schemes do not adversely affect 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, particularly since in these environments collaborative AAA Services must be deployed to allow

the user 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 the user's data must be avoided. Meeting all these requirements is complex, especially if we consider several domains. Also the resource reservation is complicated if there are several operators involved, and with respect to the handover, there are still unresolved problems in simpler networks than those proposed in a heterogeneous paradigm, as is the case of FI.

5.3. Classification based on general purposes

Table III shows that several research papers deal with the study of cryptographic mechanisms and the effect that the key length and the type (eg. symmetric or asymmetric) have on the communication delay as well as on other parameters.

Precisely, the *delay* is one of the most frequently occurring parameters in the studies analysed in Table III, followed by the *overhead*, the *throughput* and the *energy consumption*. It should to be noted that, since most of the studies analysed are based on real-time systems, the relevance of the delay parameter is understandable. In fact, in a real-time system the data received beyond a period of interest are not relevant (and usually they are discarded). Therefore, the delay is a parameter with a more negative impact in the QoS than the low throughput, for example. However, the throughput is interesting in the sense that, if the data arrives within the period of interest, ideally the maximum amount of data arrives.

In addition, *energy consumption* is a parameter that mainly concerns networks with few resources, and in particular is very important in sensor networks. Indeed, sensors are employed in order to take periodic measurements from the environment at isolated locations, so the energy consumption will determine the utility time or network lifetime.

Finally, most of the research studies here consider *performance analysis* (P.Analysis) and some of them have considered the difficulty of avoiding some attacks (particularly DoS attacks). We also found some papers where the security is explicitly identified as a parameter to protect the QoS (SfQ), while in Table I we show the opposite case, in which the QoS can be seen as a security requirement (QfS).

5.4. Considerations in the classifications

We have seen that much of the work based on *cellular networks* considers the integration of such networks with another type of technology, in particular with MANET, and proposes the use of MIP or MIH as mobility management protocols. However, there are not many studies that consider the integration between *WSN* and the rest of the networks considered, although there are several approaches that investigate the interdependencies between security and QoS (especially considering the energy factor). Regarding *MANET*, we can find in the literature both types of approaches, those that consider the Security and QoS tradeoff only in MANET, and those that consider the integration with other infrastructures, especially with cellular networks. Such a relationship is understandable because both networks can be supplemented to provide the user with a greater range of services.

Note that the information in the tables can be easily computarized and even used by Web applications in order to determine the priority between parameters prior to starting the communication with a particular network. In such cases, Security and QoS parameters can be generated independently. Indeed, it is possible to merge both types of parameters, although it is not always desirable. In most scenarios the *context* should be applied in order to determine whether either Security or QoS parameters have to be prioritized. For example, under an attack Security parameters should probably be prioritized, although it can be more complex, as we shall show in what follows.

Finally, the most common trends in the rapprochement between QoS and security are: (i) tests to evaluate the performance of new security solutions [61, 62], (ii) studies of the network QoS to help to detect the existence of threats [63, 64, 65], and (iii) security techniques to help to prevent the QoS degradation (SfQ) [66, 51, 56, 29]. Also we find studies where the QoS is considered as a prerequisite for the development of security applications (QfS) [20].

6. PARAMETRIC MODEL

In this section we define a mathematical model to show the parametric relationships between Security and QoS requirements. This model has been implemented using MATLAB and DOT files. The results show that it is possible to implement the proposed model and use it to measure the dependencies between parameters.

6.1. Dependency relationships

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 an 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 that the decrement of the first parameter affects the second parameter by decreasing its value. D^t means that the complete dependence is symmetric for both parameters.

Figure 6 shows the dependencies between performance parameters (ingot, e.g. availability), security properties

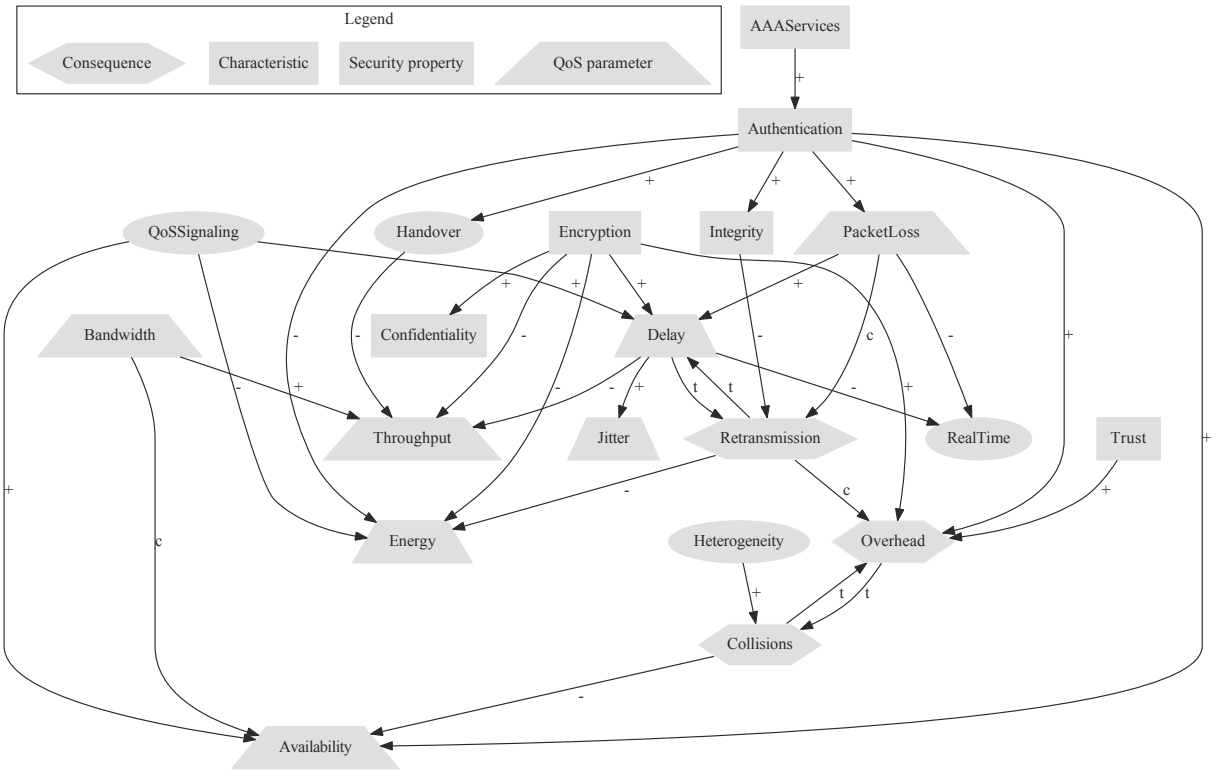


Figure 6. Parametric dependencies.

(square, e.g. integrity), characteristics of the environment (oval, e.g. to be a real-time system) and some consequences (hexahedron, e.g. collisions). Some lines are numbered indicating the relevance of such dependence regarding the rest of the 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.

Throughput might be relevant, but only once we have the two characteristics above. Moreover, *throughput* may be adversely affected by roaming scenarios, where hardening or relaxing the cryptographic mechanisms could respectively, affect it negatively or positively. This parameter is influenced by network *bandwidth*, which also affects *availability*.

Furthermore, the relationship between *QoS signaling* and *availability* should be nuanced. The QoS signaling mechanisms guarantee 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 it requires the *exchange of additional control messages* and this entails an energy consumption that may be harmful to some networks.

Also, *authentication mechanisms* may require the exchange of messages, and *encryption mechanisms* can increase the packet size to a fixed length regardless of data length. Furthermore, the execution of *cryptographic operations* adversely affects *energy consumption*. However, the authentication mechanisms can provide message *integrity*, thereby avoiding *data retransmission* and network *overload*. Moreover, the more overloaded a network is, the more likely it is to suffer *collisions*. In heterogeneous networks, collisions can occur more frequently when devices share the same communication medium. In addition, collisions damage availability by avoiding the use of the medium for data transmission. The collisions do not depend on 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 6 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 schema would be even more complex. This gives us an idea of the difficulty of developing Security and QoS tradeoff 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. This is particularly damaging in critical environments where different mechanisms that affect such parameters have to coexist.

6.2. Using parametric relationships

Figure 6 can be represented as a table, as Table IV shows. Note that we consider that the heterogeneous nature of the environment depends on the context, as the required *Bandwidth*, *Encryption* method used or the need for using QoS Signaling mechanisms, which depend on the application running in the node. Moreover, *Trust* can change over the node's lifetime. However, this sometimes depends on several factors related with the context where the node is (e.g. contact with malicious nodes).

Moreover, although we have considered a restricted set of parameters, it is possible to build complex dependency diagrams using the DOT language. For example, we used Graphviz[‡] to build Figure 6.

DOT documents are easily implemented and modified. So, building the dependencies table from the DOT document is not complex and can be easily automated. For example, we used MATLAB to implement the model proposed using DOT documents. The result using the set of parameters shown in Figure 6 is shown in Figure 7. So, Figure 7 shows the information given in Table IV once it is in the node to be used. Each square in the figure represents a relationship $X \xrightarrow{D^k} Y$.

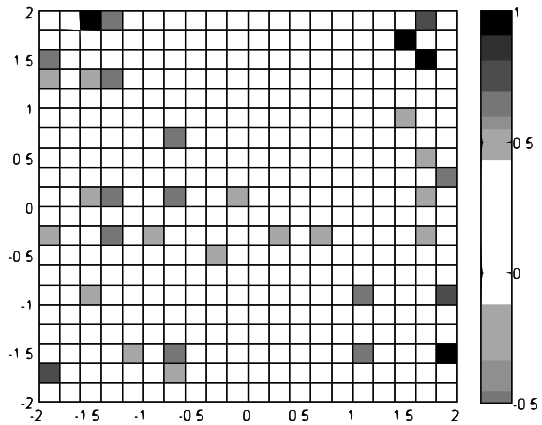
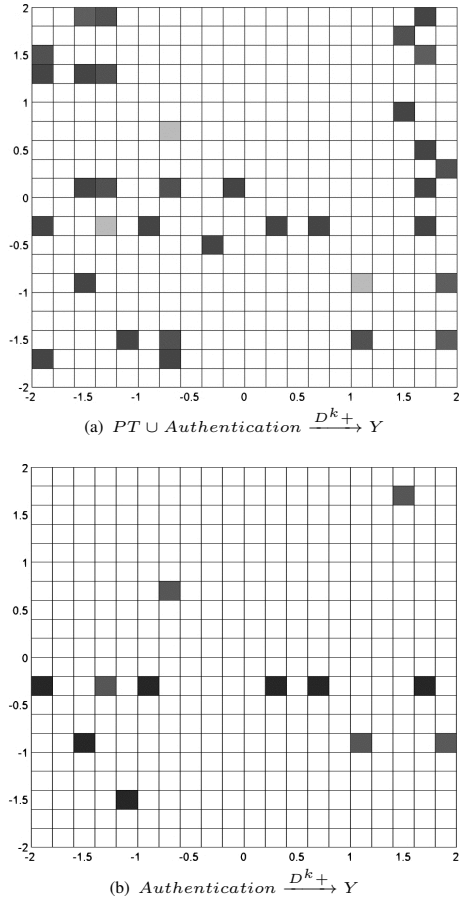


Figure 7. Parametric table.

As a consequence, the proposed model makes it possible to measure the influence of a parameter on the rest of the parameters. For example, Figure 8(a) shows how the parametric table in Figure 7 can change if just one parameter (Authentication in the example) is modified. Intuitively, when one or more parameters change their value, the global changes can be seen in the same table.

Moreover, Figure 8(b) shows only the parameters that change their values when the parameter *Authentication* changes considering the transitivity property: D^k applied once or more $(+)$, or the same as $Authentication \xrightarrow{D^k+} Y$. In addition, the whole set of parameters affected by the



(a) $PT \cup Authentication \xrightarrow{D^k+} Y$

(b) $Authentication \xrightarrow{D^k+} Y$

Figure 8. Influence of X, $X \xrightarrow{D^k+} Y$

modification of a set of parameters can be calculated by the union of multiple tables.

Figure 9 shows the opposite of the relationship shown in Figure 8(b). For example, the parameter *Authentication* only depends on the AAA Signaling parameter (in our example), which is reflected in both Figures 6 and 9(a). Whereas, if we consider transitivity, the parameter *Overhead* depends on eleven parameters: Collisions, Heterogeneity, Retransmission, Trust, Delay, Packet Loss, Integrity, Authentication, Signaling, Encryption and QoS Signaling.

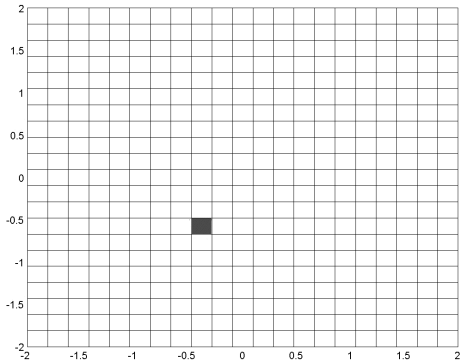
It is important to note that while in Figure 8(b) it is possible to see what parameters are directly dependent on *Authentication*, in Figure 9(b) is not possible to see the chain of parameters on which *Overhead* depends. It is not a problem, if we consider that by combining both types of tables we can find out.

Finally, in this example, the parameters Availability, Energy, Jitter, Throughput, Confidentiality and Real-Time don't affect the others. This can vary depending on the type of problem and parameters considered. For example, if we consider the number of nodes in a sensor network, then

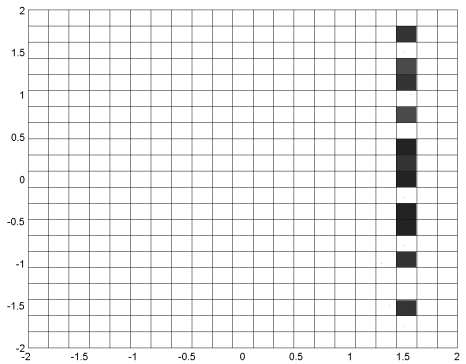
[‡] Graph Visualization Software, http://www.graphviz.org/.

Table IV. Dependencies table.

$X \xrightarrow{D^k} Y$	Availability	Bandwidth	Delay	Energy	Handover time	Jitter	Packet Loss	Throughput	AAA S.	Authentication	Confidentiality	Encryption	Integrity	Trust	Heterogenity	Real-Time	QoS S.	Collisions	Overhead	Retransmission
Bandwith	c							+												
Delay						+		-								-				t
Packet Loss			+													-				c
AAA S.										+										
Authentication	+			-	+		+						+						+	
Encryption			+	-					-		+								+	
Integrity																				-
Trust																			+	
Handover								-												
Heterogeneity																		+		
QoS S.	+		+	-																
Collisions	-																		t	
Overhead																		t		
Retransmission			t	-															c	



(a) $X \xrightarrow{D^k+} Authentication$



(b) $X \xrightarrow{D^k+} Overhead$

Figure 9. Influence on Y, $X \xrightarrow{D^k+} Y$

Energy is crucial and affects other parameters. In a sensor network, if the nodes die then the communication can be interrupted. Moreover, if we consider the configuration of computers to deliver Real-Time traffic, then the Real-Time characteristic can affect other parameters such as for example the Bandwidth, because the computer and the network have to be adapted to deliver this type of traffic.

Then, general approaches can be built taking into account a common language to implement dependencies, but there are particularities which depend on the knowledge that we have of the system and the environment.

Furthermore, one additional problem to solve here could be the storage of the dependencies in the node. It seems to be fairly intuitive that those parameters which depend on the communication with external networks belonging to different domains have to be considered too, and it could be very tiresome to store various dependency diagrams in the node, one for each type of network. There are some solutions that can be included at this point:

- The node knows *two diagrams* minimum. The first one is the parametric relationship diagram related with its native network, while the second one is the parametric relationship diagram related with the communication with heterogeneous networks.
- The node knows only the parametric relationship diagram related with its *native network* (NND). In that case, there is an *intermediary node* (IN) who knows the communication diagram. The IN adjusts the local parameters at both ends of the communication.
- The node knows only the *generic communication diagram* (GCD). In that case, the node has the basic tools to communicate in a generic environment and respects a set of parameters. However, it is not possible to optimize its behaviour.

Table V shows the advantages and disadvantages of each solution. In particular, *domain-based optimization* (DbO) is very interesting from the point of view of resource-constrained networks. For example, if a powerful node wants to use a WSN, and it uses DbO, then it could

Table V. Deployment of parametric relationship solutions.

Solution	Advantages	Disadvantages
NND+GCD	Authonomy	Storage space
NND	Domain-based optimization	Dependency from IN
GCD	Heterogeneous communication	Not domain-based optimization

adjust its parameters in order to become compatible with the foreign network.

Note that the network policies (within the context) also determine the behaviour in these cases. For example, in some networks it may be fundamental to preserve the policy " The parameters in a foreign device have to be adapted to the network properties", while in others the policy "The parameters in a foreign device have to be preserved when it is resource-constrained in contrast with local devices".

In the first case, it prevents powerless devices' malicious behaviour within a powerful network (e.g. the resource-constrained node opens a communication with a powerful node to modify its behaviour to make it less productive). In the second case, it helps to incentivize the communication between resource-constrained devices and powerful devices.

Finally, the possibilities for implementation are extremely extensive and depend on several factors. In general, the deployment of the parametric relationship solutions depends on the context where the solution is deployed and the level of autonomy required at node level.

7. OBSERVATIONS FOR INTEGRATION AND INTEROPERABILITY

In the previous sections we have explored the current state of the art for different networks considering the Security and QoS tradeoff and network interoperability. Moreover, we have presented a taxonomy that shows the most important parameters in such approaches. In this section we analyse the requirements that a system for network integration should satisfy based on the previous results. Furthermore, there are some QoS and security requirements to be considered by the network interoperability architectures in the FI. It is extremely important in order for these schemes to be effective, that possible attacks that affect the performance are avoided.

7.1. Network integration

Figure 10 shows common and specific characteristics for the three types of networks analysed.

The purpose of each network is certainly different. Thus, the *WSNs* are formed by a large number of devices that can be replaced by others of the same type, and are specialized in taking measurements from the environment in which they are placed. Furthermore, sensor networks are usually specific-purpose oriented, so they can be

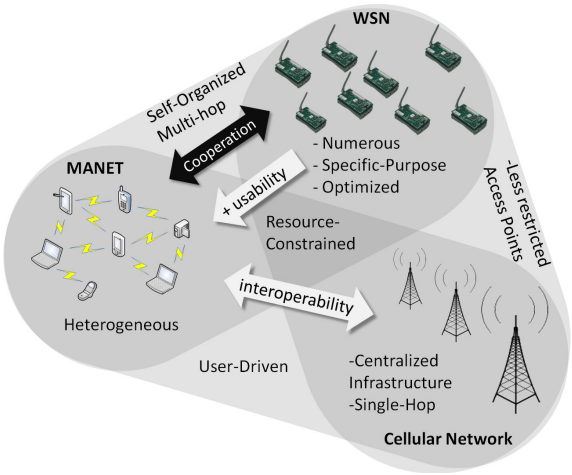


Figure 10. Network similarities and particularities.

optimized to achieve an objective efficiently (eg. to take some measurements for a specific period of time with the minimum energy consumption).

On the other hand, *MANETs* are heterogeneous networks and, therefore, add more usability and flexibility than WSNs, although both of them are self-organizing networks. However, the cost of the network being made up by different types of devices is to lose the ability to optimize resources as efficiently as a WSN. This is because in a MANET we have no prior information about the types of devices that can be interconnected (eg. terminal devices, laptops, etc.), so the hardware and the communication protocols for such devices have to be more general. So, we can conclude that the transition from WSN to MANET provides greater usability, and that the WSNs are useful for obtaining measurements from an environment efficiently.

In addition, cellular networks add advantages for the interoperability due to their centralized infrastructure that, as we have seen, can act as a gateway for the Internet access, as well as provide the infrastructure to deploy the AAA services. Both networks, MANET and cellular, are user-focused, so their interoperability could be quite attractive from a commercial point of view. Sensor networks are more specific to a particular scope, but they are optimized.

Hence, the interoperability between WSN and cellular networks could provide sensors with a way to connect to the Internet, but the BTS can be far too aggressive in terms of resource consumption (eg. consumption in data transmission) for direct use in sensor networks.

Like cellular networks, WSNs have an access point that presumably has more resources than normal devices within the network. However, even connecting these special elements to each other could have serious consequences for the QoS in WSNs, because if these devices, with more resources, use all their battery (powered off),then they could leave critical areas of the WSN without connectivity and, therefore, useless.

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 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 communicate with sensor devices (e.g. by modifying the protocol stack). However, the power consumption that a device might need to be connected to a MANET may still be too high for a sensor.

7.2. Basic requirements and observations for an interoperability scheme

Here, we present some conclusions on the possible future architectures needed to provide QoS and Security in FI. An important component for these schemes to be effective is to avoid the possible attacks that affect the performance and provide alternatives to improve the control mechanisms of the network. Furthermore, trust and privacy schemes are basic to ensure the adoption and survival of such architectures.

Figure 11 shows the main components for an interoperability scenario considering Security and QoS tradeoff within a generic node. The composition of the node will be explained in the following paragraphs. However, there is one additional consideration that we have added: the separation between static and dynamic parameters. The static parameters are those that can only be manually modified, while the dynamic parameters are dependent on the previous ones and other dynamic parameters [§]. Moreover, the context is crucial when setting the priroity between parameters and also to provide the values of some static parameters. For example, *Trust* can be considered as a dynamic security parameter, and can be local to the node. *Trust* can be dynamically modified based on other security parameters which depend on the context. Of course, *Trust* and security parameters should be stored in *antitampering* mechanisms in the device. To the contrary, additional security mechanisms should be deployed to periodically test the correctness and fidelity of the data.

Note that depending on the node resources some characteristics cannot be implemented (e.g. local IDS), although it may also depend on the implementation of the solution.

[§] This can be proved using a dependency relationship diagram such as that shown in Figure 6.

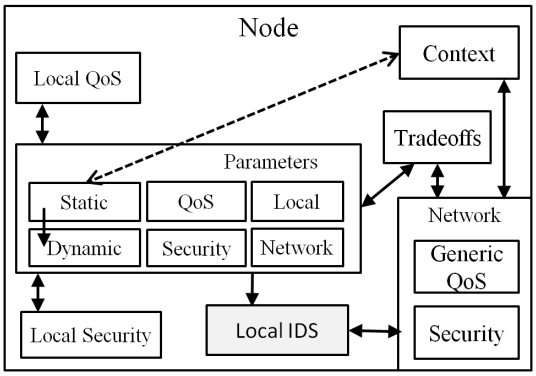


Figure 11. Security and quality of service (QoS) tradeoff components in a node

7.2.1. Quality of service.

In our approach we consider *different ways of understanding the QoS*. For example, in a WSN the QoS must be considered taking into account the lifetime of the network, and how to extend it to enable the WSN to keep working for as long as possible. Therefore, in the case of a WSN it is possible to see the network as a single service, and if we immerse ourselves in the task we can probably determine what parameters need to be considered in order to extend 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 traditional QoS mechanisms for data transmission is network congestion management. Several studies conclude that the effectiveness of such mechanisms is high in moderately congested networks, but they are useless in scenarios with low congestion and unworkable when congestion in the system is high. Therefore, after a certain 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 call these requirements the *QoS general for network convergence and interoperability*, or general QoS characteristics of the communication system.

We conclude that each network has its own QoS features that should be prioritized for their subsistence, and further more general QoS characteristics for the communication. In fact, it is possible that the QoS for the communication matches with the QoS specific for an environment, if

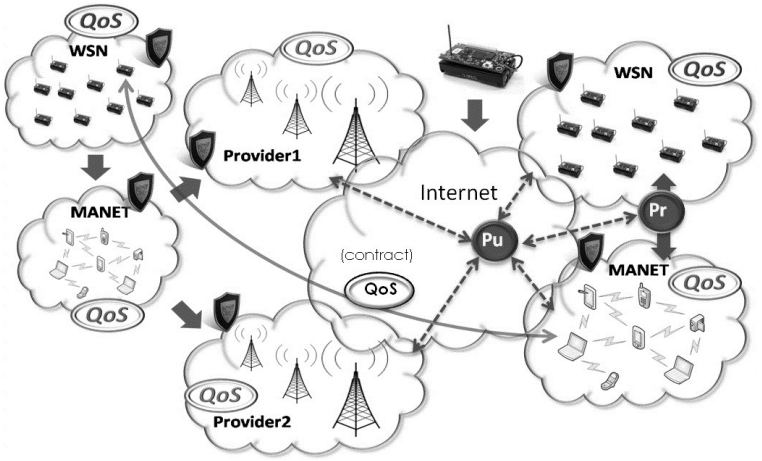


Figure 12. Cooperative security and quality of service (QoS) environment.

not, it is 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 12 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 between 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 network visited. The main objective should be that the node can enjoy the services that other networks can provide it with (e.g. Internet connection, access to environmental information, etc.) but always without interfering negatively in the QoS of the system visited. The big challenge is how to do this while *preventing nodes with fewer resources being 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.

7.2.2. Security.

As we have seen, *AAA Services* have an important role in cellular networks, but may be extensible to other networks with the aim of seeking a unified security architecture. As we have already seen in Section 3, 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 will 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 *user's data privacy*. If this happens, it might incur individual or collective lawsuits, coupled with the possible compensation expense. This could damage the reputation of the service provider.

Figure 12 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 to allow 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, avoid the traceability of information that could be analysed by unauthorized entities. *Pr* is 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 in order to enable secure cooperation between networks. The final objective is to allow both architectures to coexist and benefit each other , also increasing the collaboration between multiple paradigms.

The idea is to provide the service providers with a common infrastructure for sharing information with other networks for security purposes, and that in turn public networks can provide useful data to the system through the public architecture. The difficulty with 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 and online forums that allow users to judge and penalize misbehaviour 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.

7.2.3. Attacks that affect the performance.

Providing QoS guarantees is essential to prevent those attacks that affect the performance and which can lead to DoS. Similarly, preventing DoS attacks is fundamental to maintain QoS guarantees. Thus, 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*. Therefore, the IDS can work with the QoS mechanisms to obtain such information without generating additional traffic. This situation is shown in Figure 13. 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.

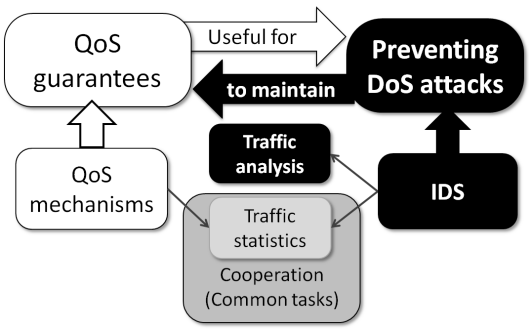


Figure 13. Avoiding additional traffic through cooperation.

The problem of attacks that affect the performance (e.g. Signalling Attacks) is that, in most cases, it is very difficult to accurately predict whether the network is under attack or, whether the network conditions are changing due to other causes, especially in *dynamic networks*. In the case of QoS mechanisms enabled to automatically react to changes in the network by varying the communication parameters to maintain the QoS guarantees, an attacker could force a change in the traffic conditions affecting the behaviour of the network, and the IDS might not realise anything has happened, since the QoS mechanisms and policies manage the network traffic.

Another possibility is that the QoS mechanisms do not act as traffic regulators and that in the case of sudden changes in the network, the IDS warns of this change (eg. to a network administrator). There are some mechanisms that can enable the IDS to *isolate* a part or the whole network in case of an attack. However, the isolation affects the availability, and for this reason automatic and reactive responses are not a good option in environments that depend heavily on this parameter. In fact, detecting and *preventing the attacks that affect the performance is a complex task that remains open to multiple interpretations*. For example, in contrast to those systems where availability is a key parameter, in other environments the priority is to prevent the data leaks, so in these systems the network isolation is an option which is more than acceptable.

Moreover, the attacks that affect performance are a big problem for network integration, since the *effect of such attacks can be propagated throughout the whole collaborative structure*. Indeed, if an attack affects any of the parameters indicated in Figure 6, then it is relatively easy to then affect the other parameters. Likewise, the attack can spread through the other networks that are connected to the infected network, producing an extremely undesirable chain reaction. However, an advantage of collaboration between networks is that, if a network that is providing a service has to be isolated, it is feasible to find another network to replace it in a short period of time. Nevertheless, a disadvantage of it is that abuse might be possible (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.

Finally, it is useful to consider the attacks that affect the performance from two viewpoints: local and network. Figure 11 shows the possibility of building a *local IDS* at the node. This solution increases the complexity of the node, but also provides local security at the node, preventing it from being misled or corrupted. The local IDS could identify when the changes in local parameters and requirements are related to each other and raise an alert or react against the probability of an attack.

However, it is not assumable that all the devices in the network have a local IDS. In such cases the IDS can be implemented by another device in the network (Network IDS). The *Network IDS* examines the network traffic and determines whether there is a threat. Intuitively, if the Network IDS can collaborate with a local IDS, it would be possible to reduce the data to be sent from the node to a external IDS (e.g. the node can send the result of computing its security state to the IDS).

Nevertheless, the way in which the local IDS is implemented in the node is fundamental to ensure it

works correctly. If the local IDS can be corrupted by the node, then the solution becomes unusable. There are anti-tampering solutions that enable storing certain data (e.g. keys, certificates) within a protected device in a node (e.g. TPM, NFC). But the problem of computing the security state while maintaining the trustworthiness of the application for it, continues to be an open challenge.

7.2.4. Trustworthiness.

Keeping trustworthiness is necessary to ensure that the restrictions imposed by the QoS application requirements are satisfied. It should be a primary objective, and therefore the control traffic dedicated to promoting or protecting this should be prioritized. Two possible implementations for introducing trust as a parameter by using the priority are based on *data stream* (DS) and *node* (IN):

- Priority based on DS. The priority of the traffic could change based on the trust level for the data stream. A data stream is a sequence of datagrams that follow the same path. Hence, the priority here would be based on the trust level of the nodes of the path (more trust implies more priority). The problem is the calculation of the priority and that, during the transmission, this priority could vary. This would entail a recalculation of priority and would complicate the architecture.
- Priority based on the IN. The idea is to assign an individual priority to the node. Thus, the source node marks the datagram with its trust level, that is used as the datagram priority. The rest of the nodes in the path should transmit the information based on this priority level.

Considering the two alternatives, the IN would be easier to implement, since the data could be sent without prior calculation of a route, and therefore does not involve additional cost for maintenance. Since priority-based transmission using the trust level as metric is too strong for data transmission (trustworthy nodes could cause overhead), this possibility could be used when the control nodes attempt to transmit high priority information about the network state (eg. IDS nodes).

7.2.5. Privacy.

The future communication mechanisms for heterogeneous networks have to consider privacy as a primary requirement, taking into account the role that the user plays in networks, as considered in our approach. So, new concepts such as *Privacy by Design* (PbD) have to be taken into account in order to look for consistency between the mechanisms developed to protect user privacy in different networks. Furthermore, future security mechanisms have to be able to avoid the traceability of users throughout the entire network. In fact, the traceability of users is directly related with privacy because it provides data to the attacker that can be analysed with the intention of discovering behaviour patterns of the user. Moreover, the user is usually exposed to these kinds of practices due to the use of services that require the acceptance of terms of service related to privacy, that are often not understood but despite this are signed by the user.

8. CONCLUSIONS

New paradigms as FI and IoT propose the interconnection of heterogeneous networks on a large scale. However, there are several issues regarding QoS and security mechanisms that have to be previously addressed. 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 order to achieve this we have selected three representative networks that will be part of the FI. These are Cellular Networks, MANETs and WSNs. In addition, we have shown a taxonomy to identify similarities between such technologies, and also to identify the requirements for network interconnection. Consequently, we have obtained parametric relationships between Security and QoS requirements. We have also proposed high-level integration architectures for those networks in the FI 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. The most appropriate way to solve these problems is the development of new security and QoS mechanisms, designed to allow interoperability between different networks. These new developments should be taken in parallel, without forgetting the current developments in different related technological areas. To reach effective convergence and interoperability, we also have to consider additional protocols to IP. In fact, although IP is a widely used protocol and is designed to be resistant against natural disasters, there is no truly effective QoS mechanism working over IP.

Moreover, as a consequence of keeping the user satisfied, the step towards allowing the use of QoS mechanisms through the Internet seems ever closer. But the real threat is that the development of such mechanisms will be carried out without taking into account the requirements of the future networks that will need them. In this case, interoperability problems may appear and the path towards cooperation will become more complex. Therefore, further steps should be taken 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 helps the Future Internet.

9. FUTURE WORK

There are several areas where the study of Security and QoS tradeoff could bring many benefits. In particular, future steps will focus on achieving Security and QoS tradeoff in critical infrastructure systems and user-dependent environments. First, WSNs play an important role in early warning systems (EWS) in the context of critical infrastructure protection (CIP). EWS are responsible for the early detection of unforeseen problems and the rapid response to these. Therefore, measuring the impact that security mechanisms have on the performance in the CIP context is of great value for the deployment, future use and maintenance of future EWS.

Second, the user being included in the environment as one more element, is very interesting from the point of view of QoS and security tradeoff. However, the impact of the user on the system is difficult to measure due to the fact they are, generally, unpredictable. However this is a key point in order to be one step closer to the Future Internet becoming a reality.

10. ACKNOWLEDGMENT

This work has been partially supported by the Spanish Ministry of Economy and Competitiveness 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.

REFERENCES

1. Najera P, Roman R, Lopez J. User-centric secure integration of personal rfid tags and sensor networks. *Security and Communication Networks* In Press; .
2. Paul Schmit GW. Mipv6: New capabilities for seamless roaming among wired, wireless, and cellular network. *Technical Report*, Intel, Developer UPDATE Magazine 2002.
3. Tsudik G. Some issues in wsn, manet and cellular security (position paper). *Proceedings of the ARO Planning Workshop on Embedded Systems and Network Security Held in Raeligh, North Carolina* 2007; .
4. Sohraby K, Minoli D, Znati T. *Wireless sensor networks: technology, protocols, and applications*. Wiley-Blackwell, 2007.
5. Akkaya K, Younis M. A survey on routing protocols for wireless sensor networks. *Ad Hoc Networks* 2005; **3**(3):325 – 349, doi:DOI:10.1016/j.adhoc.2003.09.010.
6. Noori M, Ardakani M. Characterizing the traffic distribution in linear wireless sensor networks. *Communications Letters, IEEE* aug 2008; **12**(8):554 –556, doi:10.1109/LCOMM.2008.080488.
7. Fu X, Hogrefe D, Narayanan S, Soltwisch R. Qos and security in 4g networks. *First Annual Global Mobile Congress, Shanghai, China*, 2004.
8. Khan F. *LTE for 4G Mobile Broadband: Air Interface Technologies and Performance*. Cambridge University Press, 2009.
9. Prasad A, Prasad N, ebrary I. *802.11 WLANs and IP networking: security, QoS, and mobility*. Artech House, 2005.
10. Gupta V. Ieee p802.21 tutorial. *Technical Report*, Institute of Electrical and Electronics Engineers (IEEE) 2011.
11. Stallings W. *Network security Essentials: Applications and Standars*. 3 edn., Prentice Hall, 2007.
12. Taddeo A, Ferrante A. Run-time selection of security algorithms for networked devices. *Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks*, ACM, 2009; 92–96.
13. Roman R, Lopez J. Integrating wireless sensor networks and the internet: a security analysis. *Internet Research* 2009; **19**(2):246–259.
14. Rios R, Lopez J. (un)suitability of anonymous communication systems to wsn. *IEEE Systems Journal* 2012; **PP**(99):1–13, doi:10.1109/JSYST.2012.2221956.
15. Liu J, Baek J, Zhou J, Yang Y, Wong J. Efficient online/offline identity-based signature for wireless sensor network. *International Journal of Information Security* 2010; **9**(4):287–296, doi:10.1007/s10207-010-0109-y.
16. Dietrich I, Dressler F. On the lifetime of wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)* 2009; **5**(1):5.
17. Zahariadis T, Leligou H, Voliotis S, Maniatis S, Trakadas P, Karkazis P. Energy-aware secure routing for large wireless sensor networks. *WSEAS TRANSACTIONS on COMMUNICATIONS* 2009; **8**(9):981–991.
18. Lopez J, Roman R, Agudo I, Fernandez-Gago C. Trust management systems for wireless sensor networks: Best practices. *Computer Communications* 2010; **33**(9):1086–1093.
19. Christin D, Mogre PS, Hollick M. Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives. *Future Internet* 2010; **2**(2):96–125, doi:10.3390/fi2020096.
20. Pazynyuk T, Li J, Oreku GS, Pan L. Qos as means of providing wsns security. *International Conference on Networking* 2008; **0**:66–71, doi:http://doi.ieeecomputersociety.org/10.1109/ICN.2008.22.
21. Bella G. The principle of guarantee availability for security protocol analysis. *International Journal of*

Information Security 2010; **9**:83–97.
22. Chen D, Varshney P. Qos support in wireless sensor networks: A survey. *International Conference on Wireless Networks*, vol. 233, 2004.
23. Nargunam A, Sebastian M. Self-organized qos aware multicast routing scheme for ad hoc networks. *International Journal of Computers and Applications 2010* 2010; **32**(2).
24. Roedig U, Sreenan CJ. Predictable and controllable wireless sensor networks. *Proceedings of the Information Technology & Telecommunications Conference (IT&T2005), Cork, Ireland*, 2005.
25. Sun J. Qos parameterization algorithm in data collection for wireless sensor networks. *Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks*, ACM, 2009; 57–64.
26. Yaghmaee M, Adjeroh D. A model for differentiated service support in wireless multimedia sensor networks. *Computer Communications and Networks, 2008. ICCCN'08. Proceedings of 17th International Conference on*, IEEE, 2008; 1–6.
27. Hegland A, Winjum E. Securing qos signaling in ip-based military ad hoc networks. *Communications Magazine, IEEE* november 2008; **46**(11):42 –48, doi:10.1109/MCOM.2008.4689243.
28. Zouridaki C, Hejmo M, Mark B, Thomas R, Gaj K. Analysis of attacks and defense mechanisms for qos signaling protocols in manets. *Proc. WIS Workshop*, 2005; 61–70.
29. Lu B. Quality of service (qos) security in mobile ad hoc networks. PhD Thesis, College Station, TX, USA 2005. Adviser-Pooch, Udo W.
30. Hejmo M, Mark B, Zouridaki C, Thomas R. Design and analysis of a denial-of-service-resistant quality-of-service signaling protocol for manets. *Vehicular Technology, IEEE Transactions on* 2006; **55**(3):743–751.
31. Panaousis E, Politis C, Birkos K, Papageorgiou C, Dagiuklas T. Security model for emergency real-time communications in autonomous networks. *Information Systems Frontiers Journal, Special issue on ubiquitous multimedia services* 2010; .
32. Park Y, Park T. A survey of security threats on 4g networks. *Globecom Workshops, 2007 IEEE*, 2007; 1 –6, doi:10.1109/GLOCOMW.2007.4437813.
33. Shankar R, Dananjayan P. Security enhancement with optimal qos using eap-aka in hybrid coupled 3g-wlan convergence network. *Arxiv preprint arXiv:1007.5165* 2010; .
34. Salgarelli L, Buddhikot M, Garay J, Patel S, Miller S. Efficient authentication and key distribution in wireless ip networks. *Wireless Communications, IEEE* 2003; **10**(6):52–61.
35. Al-Muhtadi J, Mickunas D, Campbell R. A lightweight reconfigurable security mechanism for 3g/4g mobile devices. *Wireless Communications, IEEE* april 2002; **9**(2):60 – 65, doi:10.1109/MWC.2002.998526.
36. Muraleedharan R, Osadciw L. Increasing qos and security in 4g networks using cognitive intelligence. *Globecom Workshops, 2007 IEEE*, IEEE, 2007; 1–6.
37. Clarke N, Furnell S. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security* 2007; **6**(1):1–14, doi:10.1007/s10207-006-0006-6.
38. Sheng Y, Cruickshank H, Pragad A, Pangalos P, Aghvami A. An integrated qos, security and mobility framework for delivering ubiquitous services across all ip-based networks. *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, IEEE; 1–5.
39. Salkintzis A, Fors C, Pazhyannur R. Wlan-gprs integration for next-generation mobile data networks. *Wireless Communications, IEEE* oct 2002; **9**(5):112 – 124, doi:10.1109/MWC.2002.1043861.
40. Bhargava B, Wu X, Lu Y, Wang W. Integrating heterogeneous wireless technologies: a cellular aided mobile ad hoc network (cama). *Mobile Networks and Applications* 2004; **9**(4):393–408.
41. Mahonen P, Riihijarvi J, Petrova M, Shelby Z. Hop-by-hop toward future mobile broadband ip. *Communications Magazine, IEEE* mar 2004; **42**(3):138 – 146, doi:10.1109/MCOM.2004.1273785.
42. Akyildiz I, Mohanty S, Xie J. A ubiquitous mobile communication architecture for next-generation heterogeneous wireless systems. *Communications Magazine, IEEE* june 2005; **43**(6):S29 – S36, doi:10.1109/MCOM.2005.1452832.
43. Cavalcanti D, Agrawal D, Cordeiro C, Xie B, Kumar A. Issues in integrating cellular networks wlans, and manets: a futuristic heterogeneous wireless network. *Wireless Communications, IEEE* june 2005; **12**(3):30 – 41, doi:10.1109/MWC.2005.1452852.
44. Saadat I, Buiati F, Cañas D, Villalba L. Overview of ieee 802.21 security issues for mih networks 2011; .
45. Ohba Y, Meylemans M, Das S. Media-independent handover security tutorial. *Technical Report*, Institute of Electrical and Electronics Engineers (IEEE) 2008.
46. Pontes A, dos Passos Silva D, Jailton J, Rodrigues O, Dias K. Handover management in integrated wlan and mobile wimax networks. *Wireless Communications, IEEE* october 2008; **15**(5):86 –95, doi:10.1109/MWC.2008.4653137.
47. Lampropoulos G, Skianis C, Neves P. Optimized fusion of heterogeneous wireless networks based on media-independent handover operations [accepted from open call]. *Wireless Communications, IEEE* august 2010; **17**(4):78 –87, doi:10.1109/MWC.2010.5547925.
48. Gutierrez PAA, Miloucheva I. Automated qos policy adaptation for heterogeneous access network environments. *Systems and Networks Communication, International Conference on* 2007; **0**:65, doi:http://doi.ieeecomputersociety.org/10.1109/ICSNC.2007.23.

49. Pérez J, Zárate V, Montes A. Geseq: A generic security and qos model for traffic priorization over ipsec site to site virtual private networks. *Next Generation Teletraffic and Wired/Wireless Advanced Networking* 2007; :175–186.
50. Fu X, Chen T, Festag A, Karl H, Schfer G, Fan C. Secure, qos-enabled mobility support for ip-based networks. *IN PROC. IP BASED CELLULAR NETWORK CONFERENCE (IPCN)*, 2003, doi:10.1.1.70.3584.
51. Cho J, Chen R. On design tradeoffs between security and performance in wireless group communicating systems. *Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on*, IEEE, 2005; 13–18.
52. Alia M, Lacoste M. A qos and security adaptation model for autonomic pervasive systems. *COMPSAC '08: Proceedings of the 2008 32nd Annual IEEE International Computer Software and Applications Conference*, IEEE Computer Society: Washington, DC, USA, 2008; 943–948, doi:http://dx.doi.org/10.1109/COMPSAC.2008.283.
53. Vivian D, Alchieri E, Westphall C. Evaluation of qos metrics in ad hoc networks with the use of secure routing protocols. *Network Operations and Management Symposium, 2006. NOMS 2006. 10th IEEE/IFIP*, 2006; 1–14, doi:10.1109/NOMS.2006.1687606.
54. Martinovic I, Zdarsky F, Bachorek A, Schmitt J. Measurement and analysis of handover latencies in ieee 802.11 i secured networks. *Proceedings of the 13th European Wireless Conference (EW2007), Paris, France*, 2007.
55. Kang D, Lee J, Kim B, Hur D. Proposal strategies of key management for data encryption in scada network of electric power systems. *International Journal of Electrical Power & Energy Systems* 2011; **33**(9):1521–1526.
56. Singh Y, Chaba Y. Security and network performance evaluation of kk'cryptographic technique in mobile adhoc networks. *Advance Computing Conference, 2009. IACC 2009. IEEE International*, IEEE, 2009; 1152–1157.
57. Trivodaliev K, Stojkoska B, Dimitrievski A, Davcev D. Evaluation issues of different cryptography algoritms in wireless sensor networks. *International Workshop on Information Security in Wireless Networks*, 2006.
58. Agarwal AK, Wang W. On the impact of quality of protection in wireless local area networks with ip mobility. *Mobile Networks and Applications* 2007; **12**(1):93–110, doi:http://dx.doi.org/10.1007/s11036-006-0009-6.
59. Yau S, Yan M, Huang D. Design of service–based systems with adaptive tradeoff between security and service delay. *Autonomic and Trusted Computing* 2007; :103–113.
60. Chen X, Makki K, Yen K, Pissinou N. Sensor network security: A survey. *IEEE Communications booktitles & Tutorials*, vol. 11, 2009; 52–73.
61. Aiache H, Haettel F, Lebrun L, Tavernier C. Improving security and performance of an ad hoc network through a multipath routing strategy. *Journal in computer virology* 2008; **4**(4):267–278.
62. Aldini A, Bernardo M. A formal approach to the integrated analysis of security and qos. *Reliability engineering & systems safety* 2006; **92**(11):1503–1520.
63. Avritzer A, Tanikella R, James K, Cole R, Weyuker E. Monitoring for security intrusion using performance signatures. *Proceedings of the first joint WOSP/SIPEW international conference on Performance engineering*, ACM, 2010; 93–104.
64. Luo H, Shyu ML. Differentiated service protection of multimedia transmission via detection of traffic anomalies. *Multimedia and Expo, 2007 IEEE International Conference on*, 2007; 1539–1542, doi:10.1109/ICME.2007.4284956.
65. Farraposo S, Owezarski P, Monteiro E. Contribution of anomalies detection and analysis on traffic engineering. *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, 2006; 1–2, doi:10.1109/INFOCOM.2006.87.
66. Askoxylakis I, Bencsáth B, Buttyán L, Dóra L, Siris V, Szili D, Vajda I. Securing multi-operator-based qos-aware mesh networks: requirements and design options. *Wireless Communications and Mobile Computing* 2010; **10**(5):622–646.