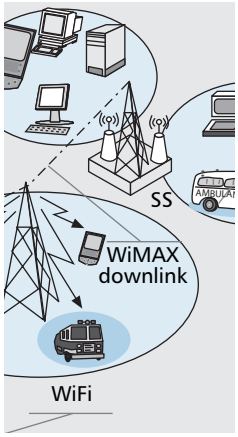
A BROADBAND WIRELESS COMMUNICATIONS SYSTEM FOR EMERGENCY MANAGEMENT

FRANCESCO CHITI, ROMANO FANTACCI, LEONARDO MACCARI, DANIA MARABISSI, AND DANIELE TARCHI



The authors discuss the main features of a wireless network that aims to interconnect several heterogeneous systems and provide multimedia access to groups of people to better monitor a specific area.

ABSTRACT

Wireless communications have received much attention during the last decades due to easy implementation, the possibility of delivering multimedia services to rural communities, and the suitability for public safety and for communicating in emergency situations. In particular, a wireless network designed for an emergency scenario must be capable of monitoring sensitive areas and must enable people to connect immediately after a disaster. This article discusses the main features of a wireless network that aims to interconnect several heterogeneous systems and provide multimedia access to groups of people to better monitor a specific area, to have a fast response in case of a disaster, and to efficiently coordinate all of the forces during the disaster management phase.

INTRODUCTION

Today, emergency management and disaster recovery systems are an issue of paramount importance in communities throughout the world [1]. An example of a suitable architecture for an efficient disaster management system is provided in Fig. 1. As we can see in this figure, the architecture is formed by the integration of three key elements: a communication infrastructure, a distributed processing environment, and a middleware layer for the integration of knowledge. In other words, the elements constituting the system architecture form a three-layer structure, where the communications infrastructure handles wireless communication among operators and connects sensor networks with the control center. The information knowledge layer forms an intermediate layer aiming to correlate all the information exchanged by the communication infrastructure, and the grid computing layer manages a distributed processing; exploiting the communication infrastructure to support decision and data mining applications.

The main goals of the disaster management system shown in Fig. 1 can be summarized as follows:

- Efficiently handle post-emergency activities with the aim of coordinating, designing, and verifying the restoration works
- Enable operations that follow a natural disaster to focus on a rapid return to normal life conditions
- Forecast and prevent further natural or man-made disasters, enabling the planning of specific monitoring activities and analysis of results arising from the monitoring campaign, and enabling access to heterogeneous networks

This article deals with the communication infrastructure layer of such a system (Fig. 1); the main aim is to provide efficient support to the information knowledge and grid computing layers by enabling reliable access to heterogeneous networks and services in a ubiquitous manner to people operating in the disaster area with different mobile devices and terminals (i.e., cellular phones, notebooks, PDAs, etc.). Attention must be focused on a two-fold requirement: to define alternative and efficient telecommunication and processing media to be deployed in a simple and efficient way in case of disaster; and to reach an efficient integration with the existing systems to provide a flexible multimedia services platform able to satisfy the manifold requirements that can arise during an emergency.

A widely accepted concept is to handle an emergency situation by resorting to a broadband communication infrastructure that must be deployed in a very short time, so as to promptly support communications among the personnel of safety and emergency agencies and to gather and elaborate the environmental data coming from monitoring devices spread in the disaster area. In addition to this, the infrastructure must be IP-based and enable interconnections with heterogeneous networks such as existing second and third generation mobile networks (global system for mobile communications [GSM], general

This work was supported in part by MIUR-FIRB Integrated System for Emergency (InSyEme) under Grant RBIP063BPH.

1536-1284/08/$25.00 © 2008 IEEE

packet radio service [GPRS], enhanced data rates for GSM evolution [EDGE], universal mobile telecommunications system [UMTS], and high-speed downlink packet access [HSDPA]), professional mobile radio (PMR) networks, IEEE 802.11 based networks, and sensor networks [2, 3].

In particular, this article focuses on an emergency communications system that uses a WiMAX-based wireless network [3] as a backbone, able to provide reliable and secure multimedia communications to operators during the disaster management phase and efficient interconnections with heterogeneous networks.

The selection of a WiMAX-based communication infrastructure is due to the fact that it groups the main required characteristics. WiMAX technology represents an optimal solution for IP-based broadband wireless communications due to its capabilities both in terms of coverage and offered data rates, as well as user mobility. Moreover, WiMAX can be easily deployed in disaster areas and enables meeting different quality of service (QoS) constraints in relation to different types of applications and traffic. In particular, in the case of an emergency communications system, it is possible to allocate network resources properly to assign priority to critical applications, such as real-time applications. Note that this is not possible, for example, in the case of basic WiFi systems that assign to all services the same level of QoS. Table 1 provides a technological comparison of WiMAX with different wireless alternatives [3], where the advantages of the WiMAX technology in terms of data rate, coverage, and user mobility are evident.

The rest of this article is organized as follows: we describe the main aspects of the WiMAX wireless network with reference to the physical layer to provide high-speed reliable communications; and QoS management to efficiently integrate different traffic types such as voice, data, video, and interconnections with heterogeneous networks. In particular, the case of the interconnection with an existing or newly deployed IEEE 802.11-based network is considered in this section. Wireless sensor networks, which are an important part of an efficient emergency communications system are considered. Some critical issues, for example, fault tolerance, are discussed in this section; and localization achieved by efficient and cost-effective implementation solutions is considered. Security aspects, which represent one of the major requirements for any emergency communications system, in particular when a disaster is due to a terrorist attack, are discussed. Suitable approaches are outlined in this section in relation to specific critical scenarios. Finally, we conclude this article.

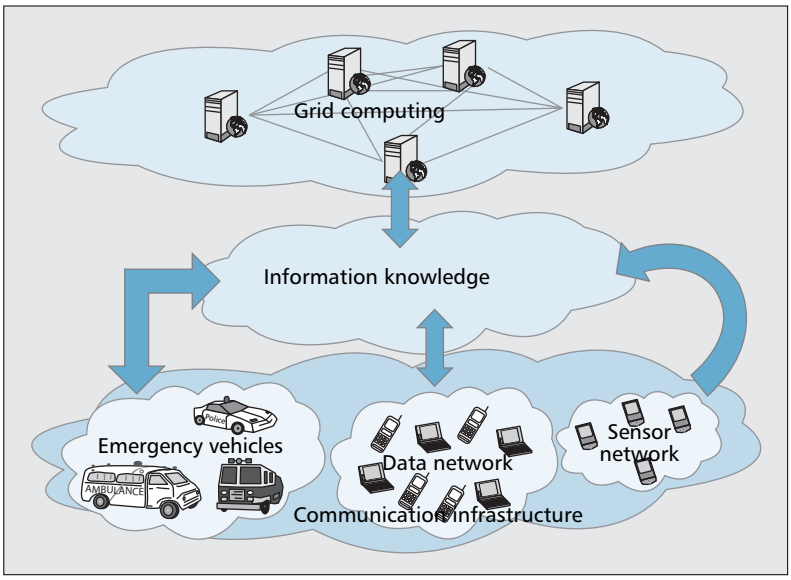


Figure 1. *Architecture of an efficient disaster management system.*

WiMAX-Based Broadband Wireless Network

Some of the most important characteristics of a typical emergency communications system are: easy implementation, full user mobility, secure and reliable communications, easy interconnection with heterogeneous networks, and high transport capacity. As stated in the previous section, among various alternatives, a WiMAX-based network seems to be the most interesting solution due to its broadband characteristics and good access/transport performance [3]. In this section, the main physical and medium access control (MAC) features of a WiMAX-based emergency communications network are dis-

Technology	Mobility	Uplink rate (Mb/s)	Downlink rate (Mb/s)	Coverage (km)	Radio technology	Spectrum type
IEEE 802.16e	100 km/h	70	70	6.5	TDD/OFDMA	Licensed Unlicensed
IEEE 802.11g	Up to 10 km/h	54	54	0.03	OFDM	Unlicensed
EDGE	Up to 250 km/h	0.474	0.474	25	FDD/TDMA	Licensed
UMTS	Up to 500 km/h	0.384	1–2	30	FDD/CDMA	Licensed
HSDPA	Up to 500 km/h	0.384	14.4	30	FDD/CDMA	Licensed
TETRA	>400 km/h	0.0072	0.0072	20	TDMA	Licensed

Table 1. *Technological comparison of wireless data standards.*

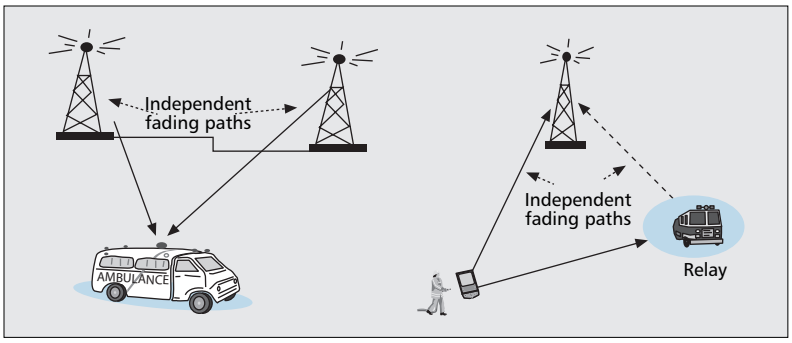


Figure 2. *An emergency scenario with MIMO-cooperative transmissions.*

cussed in relation to specific performance requirements.

In particular, to enable reliable communications with suitable QoS for different traffic types in all propagation conditions and independently of the disaster environments, for example, urban areas, underground tunnels, and so on, the WiMAX network must be optimized to provide excellent non-line-of-sight (NLOS) coverage and mobility support by using performance-enhancing technologies. Concerning the physical layer, based on the orthogonal frequency division multiple access (OFDMA) scheme, a critical aspect to be addressed is the use of efficient methods to mitigate the performance degradation due to the offset among OFDMA carriers, usually due to the local oscillator synchronization errors, and/or Doppler shift produced by the user motion within the disaster area. Carrier-frequency offset (CFO) between transmitter and receiver causes the loss of orthogonality among subcarriers and introduces inter carrier interference. In addition to an accurate receiver timing and carrier frequency synchronization for each user, the OFDMA scheme also requires a precise synchronization among all users to avoid multiple access interference (MAI), and hence system performance degradations [3]. Two methods have been proposed in the literature to counteract the MAI due to the CFO in a multiuser uplink receiver, namely, the compensation and feedback methods. The former compensates the effect of carrier frequency offsets at the receiving side to recover the ideal waveform and usually increases the implementation complexity. In the latter method, the estimated carrier frequency offsets are sent back to mobile users to adjust their transmitted signals. Despite the good performance of these approaches, to meet the severe constraints on data reliability in emergency applications, advanced CFO estimation and compensation methods must be introduced. With reference to this, an efficient approach may be that proposed in [4]. This method is based on the interference cancellation principle to counteract the effect of frequency misalignment among users. Important advantages are that additional signaling is not required, and the implementation complexity is not significantly increased.

To guarantee reliable communications, another important issue for emergency communications systems is the use of hybrid automatic repeat reQuest (H-ARQ) techniques [3]. The mean features of H-ARQ schemes are the integration of advantages of classical ARQ schemes and forward error correction (FEC) codes. H-ARQ schemes mitigate the effect of impairments due to the communication channel and external interference employing time diversity along with incremental transmission of parity codes (subpackets in this case). At the receiving end, previously erroneously decoded subpackets and retransmitted subpackets are combined to correctly decode the message. The transmitter decides whether to send additional subpackets on the basis of the received acknowledgment/negative-acknowledge character (ACK/NAK) messages.

High link reliability, wide network coverage, and high throughput are other important requirements for an emergency management system. Promising approaches to meet these requirements seem to be techniques such as transmit diversity, beamforming, and spatial multiplexing (SM) [3].

In fact, in some disaster scenarios, the particular environment can limit the number of base stations (BSs) in the area of interest and hence, higher coverage is required. In addition, the throughput could be the main requirement to be satisfied, for example, when mobile grid applications must be supported. However, in many contexts and particularly at the mobile terminals side, multiple transmit antennas are not feasible due to the limited equipment size and power consumption limitations. For this reason cooperative diversity can be an interesting solution: the basic idea is to improve the capacity of the system by means of cooperation between transmitting stations and user terminals as depicted in Fig. 2. The cooperative communities share the transmit antennas to create a virtual (distributed) antenna array and hence improve performance in terms of data reliability at the receiving end [3].

In typical emergency scenarios, frequently voice and video communications with high-rate data, as well as low-rate data communications from ambient sensors exist at the same time. By taking into account the need to handle different traffic types with different requirements in terms of delay, jitter, and error rate, suitable scheduling and resource allocation schemes can be prepared. Recently, the issue of scheduling multimedia traffic in wireless networks has become a hot research topic. Among several techniques, an efficient approach seems to be that of considering the subcarrier allocation jointly with an adaptive modulation scheme to take into account both the wireless channel behavior and specific applications requirements [5].

Important issues also to be guaranteed are high efficiency, self configuring, fault tolerance, and low delivery delay to accomplish an efficient monitoring within a disaster area and support of multimedia communications among public safety operators under critical situations. In that sense, an efficient emergency communications system must allow an easy interconnection with heterogeneous networks and support full user mobility and secure and reliable communications. To guarantee a full coverage of the disaster area,

innovative network architecture must be developed by resorting to heterogeneous mesh networking. The typical scenario includes a set of heterogeneous wireless technologies, for example, second and third generation (2G and 3G) and IEEE 802.16 and 802.11 networks. These wireless networks must be considered both in a complementary mode, that is, oriented to reach a full coverage of the disaster area, and in an alternative mode, that is, to offer to users different connection alternatives.

Because IEEE 802.11 networks are widely used, a feasible interconnection of such networks with WiMAX networks is an important issue in order to have a whole system based on IP technology with the advantage of a simpler network deployment and management; in that sense, in [6], two interconnecting techniques between an IEEE 802.11x network and a WiMAX network were proposed by taking into account the requirement of maintaining the same QoS level between the two networks, as shown in Fig. 3.

Another requirement for an emergency communications network is to support handover techniques, both intra-network (horizontal handover), that is, between areas covered by homogeneous systems, and inter-network (vertical handover), that is, between heterogeneous networks operating with different radio technologies within the communication infrastructure. Such handover mechanisms must guarantee full transparency in terms of service continuity, QoS, and security of communications. Finally, the communication infrastructure must guarantee secure and reliable communications between operators during all the phases of the rescue operation. In this case, as highlighted later, the attention must be devoted to access authentication procedures that must guarantee the seamless access to any wireless infrastructure available at the point in which the user is located at the access request instant.

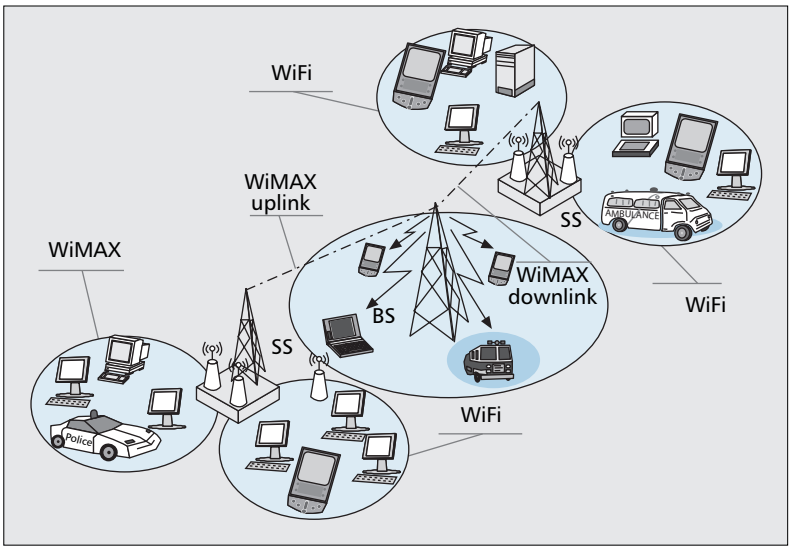


Figure 3. *A heterogeneous WiFi-WiMAX network.*

Safety Monitoring with Wireless Sensor Networks

An efficient and effective monitoring of phenomena occurring in a certain area is a key issue to prevent or to manage further risks. This is the case of wide-area scenarios where no infrastructures were available even before a disaster occurred, such as earthquake, seaquake, or flooding zones. Wireless sensor networks (WSNs) have introduced a novel paradigm for reliable monitoring [7], and they seem to be an interesting approach for many emergency situations. WSNs outperform conventional sensor systems that usually require large, expensive *macrosensors* that must be accurately placed and *wired* to the remote control center. In particular, WSNs can contain a great number of spatially separated nodes, with increased coverage and accuracy, and without requiring human attention. Moreover, WSNs can be deployed in almost any environment, especially in risk and inaccessible zones, such as in the place where a disaster happened (earthquakes, eruptions, flooding, forest or urban fires) or in the proximity of a possible hazard (volcanoes, faults, epidemics, nuclear power stations). As a consequence, one of their mean expected features is the reliability in data acquisition/transmission, robustness with respect to faults [8, 9], and capability to interoperate with heterogeneous *ad hoc* deployed networks.

For WSN applications in a typical emergency scenario, data must be delivered reliably over the noisy, error-prone, and time-varying wireless channel. To improve the reliability of the decision making process (layer two in Fig. 1), a robust air interface must be adopted for remote data delivering (i.e., from gateway to server); to this end, the IEEE 802.16e technology seems to be a good candidate [3].

In addition, sensors also are prone to fail. Faults in WSNs are not an exception and tend to occur frequently, due to energy shortages and the occurrence, in special scenarios, of *denial of service* attacks, that is, the result of any action that prevents any part of a WSN from functioning correctly or in a timely manner. As a consequence, *fault tolerance* is an important issue for applications within an emergency communications system to avoid system failures, while continuing to collect and deliver reliable information to the control centre (*survivability*). It is worth noting that, despite the fact that WSN hardware platforms and communication protocols are usually low-power designed, the critical application requirements often require a low latency data delivery to enhance the interaction degree. As a consequence, power constraints must be relaxed and the possibility of turning off nodes must be taken into account even in the case of rescue operations of a short duration.

A rough solution to this problem, at the expense of an increased cost, is to resort to redundant deployment of sensors and replication of information between sensor nodes. However, a trade-off always exists between minimizing the cost to keep the system affordable and improving system reliability by adding system components for redundancy and management purposes. An alternative approach consists in making the *whole* system capable of performing self-testing, self-calibrating, self-maintaining, self-protecting,

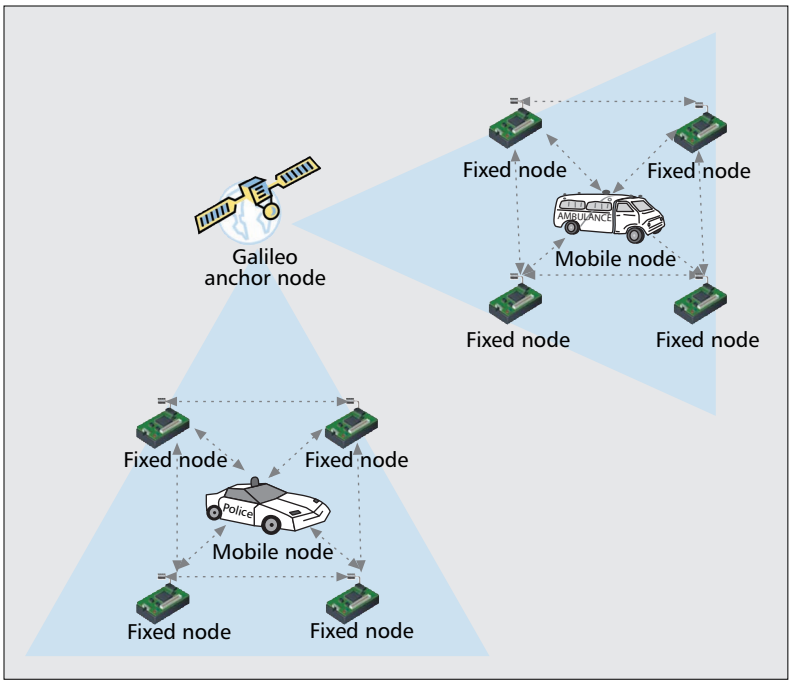


Figure 4. *Mobile node localization.*

self-healing, self-repairing, and self-recovery procedures during their lifetime in a *cooperative* way. In particular, an ad hoc multihop architecture allows a high degree of flexibility, though a trade-off between delay and information accuracy must be achieved through collaboration among sensors.

In the majority of applications, failure detection is vital not only for fault tolerance, but also for the *safety* of people working or living in the area, in particular, after a terroristic attack. In addition to detecting a failure, it is necessary to gather indications useful to determine the origin and the type of attack and consequently, to alert the remote control center.

With the aim of achieving a robust network architecture, providing a fault tolerant communications support for emergency applications with WSNs, a suitable approach is to resort to a solution based on a *tiered architecture*. In particular, a two-tier topology is applied to enhance scalability and efficiency of communications protocols. According to this topology, after a cluster has been established through a *set-up* procedure, ordinary nodes (ONs) are continuously monitored by their own cluster head (CH) that is also in charge of remote data delivering. Whenever, an abnormal operative condition — due to link quality variation — is detected, a warning is sent to the control center and if the problem still occurs, the involved ONs are assumed to be definitely lost and as a consequence, the CH manages an *orphanage* procedure to recover the ONs. However, if no CH is available, a group of ONs jointly adopts a *multihop* routing strategy, setting up a sort of ad hoc network to reach the remote server.

Location Aware Applications

Localization of sensors, network nodes, and user terminals within an operative area is one of the key issues for the communication infrastructure layer for the disaster management system shown in Fig. 1. For example, within a health emergency care scenario, the position of the possible victims must be established to coordinate the rescue operation; or in managing a hurricane response, it is useful to identify the disaster scenarios and set up alternative transportation or communication solutions relating to an evacuation plan. To meet the typical requirements of an emergency communications system, a localization protocol must be:

- Robust to node failures
- Insensitive to measurement noise
- Low error in location estimation
- Flexible in any terrain

Concerning the latter requirement, because an emergency can occur indifferently in both in indoor and outdoor environments and even in an intermediate scenario in which buildings are critically damaged, an optimal localization approach must be able to dynamically adapt to the channel features.

Currently, two types of localization techniques address these challenges: *beacon*-based and *relative location*-based [10]. Both techniques can use range and angle estimations for sensor node localization through received signal strength (RSS), time of arrival (TOA), time difference of arrival (TDOA), and angle of arrival (AOA).

Localization methods suitable for applications in emergency situations seem to be those based on beacons with a field containing the known sender position. This ad hoc inspired localization system requires that a few nodes know their location (*anchor* nodes), for example, by means of satellite systems, like a global positioning system (GPS) or Galileo (Fig. 4).[1] This enables nodes to discover their location through a two-phase process: *ranging* and *estimation*. During the ranging phase, each node estimates the distance from its neighbors. The estimation phase then enables neighbors to use the range estimated in the ranging phase and the known position of the anchor nodes to estimate their locations. To overcome the typical limitations of the *range-based* localization schemes, due to the outage of the underlying localization process, many *range-free* solutions have been proposed, based on the location information hop-by-hop, relayed from the source to the sink. These solutions estimate the location of sensor nodes or user terminals by exploiting the radio connectivity information among neighboring nodes, or the sensing capabilities that each sensor node possesses; in any case, the sensor nodes must collaboratively work together to assist each other. Due to the specific characteristics of these approaches, the range-free localization can be divided into anchor-based schemes that assume the presence of sensor nodes in the network, with known position, and anchor-free schemes that require no special sensor nodes for localization. The range-free localization schemes eliminate the requirement for high-cost specialized hardware on each sensor node. Because radio propagation characteristics vary over time and are environment dependent, higher calibration costs for the anchor-based localization schemes are imposed.

Based on the fact that each type of localization protocol offers different capabilities, future sensor network applications are expected to rely on a combination of localization techniques.

A novel approach to provide reliable localization information and reduce the implementation cost was recently proposed [11]. The basic idea is to implement smart nodes cooperation for the sake of cost minimization and to face satellite signal faults or *outage*, occurring especially within an *indoor* environment, as in the case of rescue operations inside buildings or tunnels.

In particular, in the basic approach (called satellite alone [SA]), only one device is assumed to be equipped with a satellite receiver on board, namely, a satellite node (SN), with enhanced processing capabilities with respect to the other ones. The remaining nodes can localize themselves by means of information sent from a *mobile* SN, evaluating the mutual distance through the relative RSS. With the aim of facing possible problems, a hybrid localization protocol was introduced that resorts not only to ranging packets originated by an SN, but also to those sent by location aware nodes (LANs), called in-ranging (IR). Compared to an SA solution, the introduction of an IR procedure provides two benefits:

- Obtaining a *coarse grain* and quicker localization to support critical applications
- Reducing the algorithm complexity in terms of both the paths of a mobile SN and the packets sent in the network with *lower overhead*

An IR approach might be successfully applied whenever the SN cannot cover the entire deployment area or it is out-of-service due to malfunctioning or satellite system outage, especially in indoor environments. This might be the case of managing a rescue team (fire or police brigades) operating within a damaged building, a tunnel, or a forest. In both circumstances, the LANs (even if they received only three ranging packets) might be able to perform the IR procedure. Each node that becomes a LAN broadcasts an IR-packet containing its estimated position and the transmitted power level. The IR packet is then processed as if it is an SN ranging packet to estimate its own position. Therefore, a node can utilize IR and SN packets indifferently, even if IR positioning measurements are less accurate than those provided by an SN. Of particular interest, this allows a *seamless* scenario transition in practical applications of an emergency communications system.

Security Considerations

Availability and robustness of the network are fundamental issues for any rescue operation. Moreover, if the emergency is caused by human factors (e.g., terrorism or criminal actions), security services such as privacy, authentication, or access control achieve paramount importance. As a consequence, in emergency communications systems, a fundamental requirement is that the network must be reliable and secure against attacks performed by malicious entities. The scenario outlined so far offers a great challenge in the security field, mainly due to three factors: the heterogeneity of the network, its distributed nature, and the requirement of strictly real-time communications. In this section, we discuss each of these factors and their impact on security for emergency communications systems.

Heterogeneity

The devices that usually operate within a disaster area are different, both in terms of the protocols used and the hardware capacity. Despite this, end-to-end communications between entities involved in the rescue operations must be secure. As an example, we can consider the case of data initially acquired by a sensor node, successively conveyed along a multihop sensor network, then routed to a WiMAX access point, and finally delivered to a remote control center using the WiMAX backbone network. Although IEEE 802 network security is based on digital certificates, this technique is not applicable to wireless sensor network devices due to their limited hardware capability, so the heterogeneity of the system does not permit the use of a single security method; however, each of these networks contains its specific security services, such as access control or data authentication.

Even if the single algorithms may be different, the security services are generally the same, so that the definition of proper inter-working system (IWS) functions between the security stacks of each communication media can help interoperability. IWS functions are required so that the information coming from a WSN using certain security services are matched with equivalent services on the backbone network using a different security stack.

Distribution

As mentioned previously, a static hierarchical network is not a suitable instrument to face the highly dynamic scenario of emergency interventions. A distributed network is more flexible and can be reconfigured automatically without the requirement of a centralized manager. However, from the point of view of security, the lack of a fixed structure introduces more security challenges. Most of the authentication and access control protocols are based on the presence of a centralized authentication server, but if this server is not always reachable, trust relationships between nodes must be assured using distributed algorithms or protocols based on the delegation of responsibility. Efficient distributed authentication algorithms for applications in emergency communications systems are an active field of research.

Real-Time Communications and Mobility

Emergency communications systems often transport data with stringent time constraints, such as voice, video, or software calls to remote systems. Security protocols introduce an overhead in terms of packets exchanged and computational complexity that can conflict with these constraints. As an example, IEEE 802.11/ WiMAX-based networks require a complete

A distributed network is more flexible and can be reconfigured automatically without the requirement of a centralized manager. However, from the point of view of security, the lack of a fixed structure introduces more security challenges.

Emergency communications systems often transport data with stringent time constraints, such as voice, video, or software calls to remote systems. Security protocols introduce an overhead in terms of packets exchanged and computational complexity that can conflict with these constraints.

re-authentication of the terminal with the centralized authentication server when performing handovers. This procedure might involve the exchange of several packets and verification of digital signatures, so it gives rise to significant service degradation in terms of delivering delay; this situation is made even worse for vertical handovers, when security procedures must be bridged between multiple.

As two practical examples of challenges introduced by security requirements, we describe two real case open issues and solutions suggested in the literature. The first scenario is represented by IEEE 802.11 wireless mesh networks: in these kinds of networks, the authentication is based on the presence of a centralized authentication server, reachable with the Extensible Authentication Protocol (EAP) and the Remote Authentication Dial-In User Service (RADIUS) protocol. Whatever authentication method is applied (shared key, transport layer security [TLS], etc.), at least a four-way handshake between the roaming node and the server is required. This overhead makes the network non-scalable by the number of nodes; and computationally heavyweight authentication protocols, such as TLS, can overload a single server. In [12], the problem was analyzed, and a solution was proposed based on the reduction of the number of packets required for re-authentication opposed to the first complete authentication, which is applicable in realistic networks.

The second issue is key-establishment and eventually, authentication in WSNs. This field is very active and has produced interesting solutions, because the lack of hardware capabilities must be balanced with innovative use of low-cost crypto primitives. In such a field, original schemes for pre-distribution keys or the use of functions that can approximate the behavior of public/private key schemes (such as multivariate polynomials) are under active research, although far from standardization. WSNs are still perceived as dedicated networks where ad hoc solutions are applied to each specific need, and no generic security procedure is present now.

Conclusion

This article has presented a wireless infrastructure designed for an emergency scenario having the possibility of monitoring sensitive areas and enabling intercommunication between all of the people working immediately after the disaster strikes. The key parts of such wireless infrastructure, that is, the WiMAX-based, broadband, wireless network and the wireless sensor network for ambient monitoring, were described. Suitable solutions were highlighted in order to achieve high and reliable performance in different disaster scenarios. Special attention was devoted to issues such as heterogeneous network interconnection, full and fault tolerant coverage of the disaster area, localization to enable an efficient coordination of the rescue operations, and finally, security, which represents one of the major requirements for an emergency communications system, in particular, when a disaster is due to a terrorist attack.

References

[1] L. E. Miller and Z. J. Haas "Public Safety," *IEEE Commun. Mag.*, vol. 44, no. 1, Jan. 2006, pp. 28–29.
[2] A. K. Salkintzis, "Evolving Public Safety Communication Systems by Integrating WLAN and TETRA Networks," *IEEE Commun. Mag.*, vol. 44, no. 1, Jan. 2006, pp. 38–46.
[3] L. Nuaymi, *WiMAX Technology for Broadband Wireless Access*, Wiley, June 2007.
[4] D. Marabissi, R. Fantacci, and S. Papini, "Robust Multiuser Interference Cancellation for OFDM Systems with Frequency Offset," *IEEE Trans. Wireless Commun.*, vol. 5, Nov. 2006, pp. 3068–76.
[5] G. Song and Y. G. Li, "Utility-Based Resource Allocation and Scheduling in OFDM-Based Wireless Broadband Networks," *IEEE Commun. Mag.*, vol. 12, no. 12, Dec. 2005, pp. 127–34.
[6] R. Fantacci and D. Tarchi, "Bridging Solutions for a Heterogeneous WiMAX-WiFi Scenario," *J. Commun. and Networks*, vol. 8, no. 4, Dec. 2006, pp. 369–77.
[7] F. Akyildiz *et al.*, "Wireless Sensor Networks: A Survey," *IEEE Comp. Networks*, vol. 38, Mar. 2002, pp. 393–422.
[8] A. Hać, *Wireless Sensor Networks Designs*, Wiley, 2003.
[9] M. Ilyas and I. Mahgoub, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press, 2005.
[10] F. Chiti and R. Fantacci, "Wireless Sensor Network Paradigm: Overview on Communication Protocols Design and Application to Practical Scenarios," *EURASIP Newsletter*, vol. 17, no. 4, Dec. 2006, pp. 6–27.
[11] F. Chiti *et al.*, "Cooperative Localization Protocols for Wireless Sensor Networks," *Proc. IEEE GLOBECOM '07*.
[12] L. Maccari *et al.*, "Secure, Fast Handoff Techniques for 802.1X-Based Wireless Network," *Proc. IEEE ICC '06*, vol. 9, June 2006, pp. 3917–22.

Biographies

FRANCESCO CHITI [M'01] received a degree in telecommunications engineering and a Ph.D. degree in informatics and telecommunications engineering from the University of Florence in 2000 and 2004, respectively. His current research is devoted to link and network layer protocol design for ad hoc and sensor networks. He took part in several European research projects, such as IP GoodFood, STREP DustBot, NoEs NEWCOM, CRUISE, GJU TWIST, ETSI STF179, and COST 289 action.

ROMANO FANTACCI [F'05] is a full professor at the University of Florence, Italy. His current research interests are digital communications, computer communications, and wireless broadband communications networks. He received the IEE IERE Benefactor premium in 1990 and the IEEE ComSoc Award for Distinguished Contributions to Satellite Communications in 2002. He is currently serving as Associate Editor for *Telecommunication Systems*, *International Journal of Communications Systems*, and *IEEE Transactions on Communications*; and Area Editor for *IEEE Transactions on Wireless Communications*.

LEONARDO MACCARI graduated from the Engineering School of the University of Florencewith a degree in computer engineering in 2004. He joined the Electronic and Telecommunications Department in 2005 as a research fellow. His current research interests are security aspects of wireless telecommunications, with special focus on mesh, sensor, and P2P networks.

DANIA MARABISSI [M'00] received a degree in telecommunications engineering and a Ph.D. degree in informatics and telecommunications engineering from the University of Florence in 2000 and 2004, respectively. She joined the Electronic and Telecommunications Department at the University of Florence in 2000, where she now works as a research assistant. She currently conducts research on physical layer design for spread-spectrum wireless systems. In particular, her interests include OFDM, multiple access technique, multi-user detection, and channel estimation in broadband wireless communications.

DANIELE TARCHI [S'98, M'06] received an M.S. degree in telecommunications engineering and a Ph.D. degree in informatics and telecommunications engineering in 2000 and 2004, respectively, from the University of Florence, Italy, where he is now an assistant professor. His research interests are in both physical and data link layers, with particular interests in link adaptation, adaptive modulation and coding techniques, resource allocation, and WiMAX and OFDMA networks.