7

The Role of WiMAX Technology in Distributed Wide Area Monitoring Applications

Francesco Chiti, Romano Fantacci, Leonardo Maccari, Dania Marabissi and Daniele Tarchi

7.1 Monitoring with the WSN Paradigm

Wireless sensor networks (WSNs) represent an inherently disruptive approach specifically designed to detect events or phenomena, collect and process related data, and transmit sensed information to final users in a distributed way (Akyildiz *et al.*, 2001).

Although WSNs exhibit several features common to wireless *ad hoc* or mesh networks, such as self-organizing capabilities or short-range broadcast communication with a multihop routing, they present additional constraints in terms of limitations in energy, transmit power, memory and computing power. Further, the operative conditions usually require cooperative efforts of sensor nodes in the presence of frequently changing topology due to fading and node failures or node mobility (Ilyas and Mahgoub, 2005).

A typical WSN is comprised of the following basic components:

- A set of distributed or localized sensors;
- An interconnecting network usually, but not always, wireless-based;
- A central point of information clustering;
- Computing resources at the central point (or beyond) to handle data correlation, event trending, status querying and data mining.

WiMAX Evolution: Emerging Technologies and Applications Edited by Tsutomu Ishikawa
© 2009 John Wiley & Sons, Ltd. ISBN: 978-0-470-69680-4

These elements allow a system administrator to observe and react to events and phenomena in a specified environment. The administrator can be a civil, governmental, commercial or industrial entity. Typical application fields can span from agriculture (AgroSense, 2007–2010, GoodFood, 2004–2006) and environmental monitoring (DustBot, 2007–2009), civil engineering, disaster management (InSyEme, 2007–2010), military applications up to health monitoring and surgery (Chiti and Fantacci, 2006).

Generally speaking WSN systems can be classified into two basic categories:

- Mesh-based systems with multihop radio connectivity between WSNs, utilizing dynamic routing in both the wireless and wired portions of the network.
- Point-to-point or multipoint-to-point (*star-based*) systems generally with single-hop radio connectivity to WSNs, utilizing static routing over the wireless network.

The latter scheme is composed of networks in which the end devices (i.e. the sensors) are one radio hop away *forwarding node*, for example, a wireless router connected to the terrestrial network via either a wired or a point-to-point wireless link. On the other hand, the former approach allows end devices (sensors) to be more than one radio hop away from a routing or forwarding node. The forwarding node is a wireless router that supports dynamic routing, while wireless routers are often connected over wired links covering a wider area.

Presently WSNs have been largely focused on dense, small-scale homogeneous deployments to monitor a specific physical phenomenon. Nevertheless, the integration of multiple heterogeneous sensor networks operating in different environments could provides the ability to monitor diverse physical phenomena at a global scale, as addressed in WP122 (2008). In addition, such remote integration will make the infrastructure able to query and fuse data across multiple, possibly overlapping, sensor networks in different domains. Moreover, new types of sensor networks based on *mobile sensor platforms* are becoming available, for example, vehicles in the urban grid or firefighters in a disaster recovery operation equipped with a variety of sensors (Ilyas and Mahgoub, 2005, InSyEme, 2007–2010) (location, video, chemical, radiation, acoustic, etc). The vehicle grid then becomes a sensor network that can be remotely accessed from the Internet to monitor vehicle traffic congestion and to prevent accidents, chemical spills and possible terrorist attacks. Likewise, on-site operators as firefighters might be equipped with several wearable devices such as cameras or sensors, allowing the commander to be aware of the conditions in the field and to direct the operations to maximize the use of the forces, while preserving the life of his responders.

As a consequence, one of the most interesting applications of an integrated WSN is the ability to create a *macroscope* to take a look at a picture of the monitored environment wider than the areas monitored by a single WSN (WP122, 2008). There have been several attempts, for instance, the WSN deployed on redwood trees, a wildlife monitoring site on Great Duck Island, tracking zebras in their natural habitat and monitoring volcanic eruptions. All of these systems have been deployed in remote locations with limited access: some areas might be accessible only once in several months, straining the lifetime of sensors with limited battery power. Many are subject to harsh elements of nature that cause rapid device and sensor malfunction. Network links to back-end monitoring and collection systems may be intermittent due to weather or other problems, while in-network data storage is limited, leading to important observations being missed.

In addition to this, there is an increasing interest in real-time connecting heterogeneous devices with application to building/commercial automation (security, lighting control,

access control) or industrial control (asset management, process control, environmental, energy management). These applications usually addressed as *invisible computing* involve different technologies such as (WPANs: Wireless Personal Area Networks in which IEEE 802.15.4/ZigBee standard plays a crucial role), Wireless Local Area Networks (WLANs; mainly IEEE 802.11a/b/g/h, etc. standards) and metropolitan transport (for which IEEE 802.15.3/WiMAX standards are ideally suited).

For the aforementioned applications, the sensor networks cannot operate in a stand-alone manner; there must be a way to monitor an entity to gain access to the data produced by the WSN. By connecting the sensor network to an existing network infrastructure such as the global Internet, a local-area network, or a private Intranet, remote access to the sensor network can be achieved. Given that the TCP/IP protocol suite has become the *de-facto* networking standard, not only for the global Internet but also for local-area networks, it is of particular interest to look at methods for interconnecting sensor networks and IP core networks. Sensor networks often are intended to run specialized communication protocols, for example IEEE 802.15.4 or Zigbee, therefore an all-IP-network will not be viable, due to the fundamental differences in the architecture of IP-based networks and sensor networks. It is envisaged that the integration of sensor networks with the Internet will need gateways in most cases. A proxy server at the core network edge is able to communicate both with the sensors in the sensor network and hosts on the TCP/IP network, and is thereby able to either relay the information gathered by the sensors, or to act as a front-end for the sensor network. It is also envisaged that sensing devices will be equipped with interfaces to wireless access networks such as 2/3G and WLAN enabling total *ubiquitous connectivity*.

7.2 Overall System Architecture

As discussed previously, a wide area WSN could be achieved by integrating specialized and even heterogeneous subnetworks through a reliable transport backbone. For many kinds of applications a wireless connection represents a flexible and cost-effective solution. In particular, the Worldwide Interoperability for Microwave Access (WiMAX), provides wireless broadband services on the scale of the Metropolitan Area Network (MAN). WiMAX brings a standards-based technology to a sector that otherwise depends on proprietary solutions: the standardized approach ensures interoperability between WiMAX equipment from vendors worldwide reducing costs and making the technology more accessible. This technology can provide fast and cheap broadband access in areas that lack infrastructure (fiberoptics or copper wire) such as rural areas, unwired countries and disaster recovery scenes where the wired networks have broken down (WiMAX can be used as backup links for broken wired links). Very often WSNs are used in these areas to monitor the environment, to prevent natural disasters or to aid rescue operations. WiMAX can also provide the last mile coverage in urban areas where the monitoring and control of anthropic processes taking place, including buildings, streets, factories and storehouses. WiMAX attributes open the technology to a wide variety of applications: with its wide coverage range and high transmission rate, WiMAX can serve as a backbone for integrating specialized sensors subnetworks and for connecting the WSN to the data processing center. Alternatively, users can connect mobile devices such as laptops and handsets directly to WiMAX base stations; WiMAX is able to support vehicular speeds of up to 125 km hour^{-1} providing ubiquitous

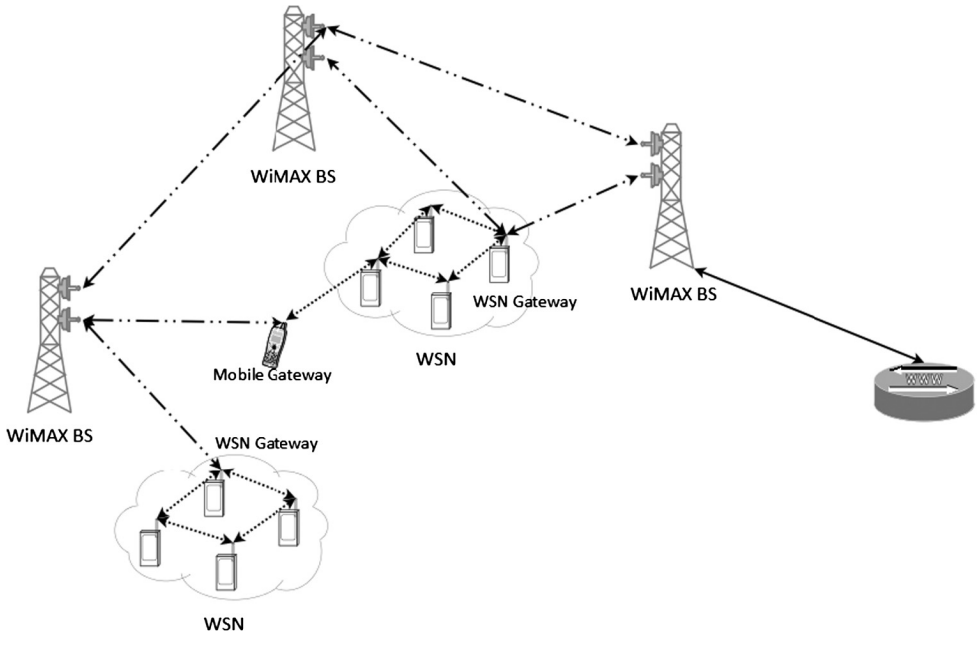

Figure 7.1 Envisioned system architecture providing interoperability among nonoverlapping WSNs through mesh-based WiMAX backhaul, as well as supporting mobile data mule.

mobile services. In this way the information coming from the WSNs can be distributed to the users: a user may be using a wireless videophone, a laptop or a PDA to access data while also dynamically interacting with the remote server by means of additional content uploading regarding a monitored area. For example, a fire team could download the internal map of a building to support or enhance the localization information coming from the WSN.

The IEEE 802.16 standard was designed mainly for point-to-multipoint topologies, in which a base station distributes traffic to many subscriber stations but it also supports a *mesh mode*, where subscriber stations can communicate directly with one another. The latter mode allows the Line-of-Sight (LOS) requirement to be related and the deployment costs for high-frequency bands to be eased by using subscriber stations to relay traffic to one another. In addition the use of multihop relay stations can extend the coverage area and improve throughput at a feasible economical level. The mesh mode can be a feasible solutions to connect distributed WSNs that must be connected together or to the same data processing center.

A possible architecture enabling the integration of heterogeneous WSNs, is depicted in Figure 7.1.

In addition to the previous advantages the choice of WiMAX technology is based on its Physical (PHY) and Medium Access Control (MAC) features that make a reliable, flexible and secure wireless system. The IEEE 802.16 MAC layer supports Quality of Service (QoS) for stations through adaptive allocation of the uplink and downlink traffic. This is very important to manage different data flows provided by different WSNs. In addition the security

sublayer provides functionalities such as authentication, secure key exchange and encryption assuring the WSNs data is not corrupted. The MAC of 802.16 supports different transport technologies such as Internet Protocol version 4 (IPv4), IPv6, Ethernet, and Asynchronous Transfer Mode (ATM) making the integration of heterogeneous networks easier.

Finally, PHY layer is characterized by a high level of flexibility in the allocated spectrum. the work frequency can be chosen to improve performance and interference and the bandwidth can be varied depending on the requirements (i.e. IEEE 802.16e uses the Scalable Orthogonal Frequency Division Multiple Access (S-OFDMA) scheme). The adaptive features at the PHY allow trade-offs between robustness and capacity and the robustness to the adverse propagation conditions permits the use of Non-Line-of-Sight (NLOS) communications, differently from alternative technologies currently available for fixed broadband wireless supporting only LOS coverage.

7.3 Efficient Access Management Schemes

As stated in the previous section, WiMAX represents a promising and reliable solution to provide a transport backbone among sensor subnetworks. As a matter of fact, it allows the establishment of effective communications handling different data flows with specific QoS requirements in terms of priority level, throughput, delay and jitter as well. The dynamic and flexible resource allocation scheme WiMAX is able to support typical application features concerning, for instance, the monitoring of synchronous processes, dispatching warnings and alarms and the reliability of data exchange.

The IEEE 802.16 family of standards (IEEE, 2005, 2004), supported by the WiMAX commercial consortium, defines the PHY and MAC layers specifications for a Broadband Wireless Access (BWA) communication protocol. Both MAC and PHY are designed to have a flexible access scheme and an adaptive resource management. This aspect is very important in the proposed architecture to manage a high number of distributed users including sensors subnetworks also under mobility conditions.

As for the PHY layer, among several alternatives, the IEEE 802.16 standard proposes the use of Orthogonal Frequency Division Multiplexing (OFDM) for mitigating frequency-dependent distortion across the channel band and simplifying the equalization in a multipath fading environment (van Nee and Prasad, 2000). The basic OFDM principle is parallelization: by dividing the available bandwidth into several smaller bands that are called subcarriers, the transmitted signal over each subcarrier may experience flat fading. Moreover, Orthogonal Frequency Division Multiple Access (OFDMA) is used to provide a flexible multiuser access scheme: disjunctive sets of subcarriers and OFDM symbols are allocated to different users.

To have more flexible and efficient OFDM/OFDMA systems, adaptive OFDM schemes are adopted to maximize the system capacity and maintain the desired system performance (Bohge *et al.*, 2007, Keller and Hanzo, 2000b). In particular, in an OFDM-based wireless system, the inherent multi-carrier nature of OFDM allows the use of link adaptation techniques according to the behavior of the narrow-band channels: the bit-error probability of different OFDM subcarriers, transmitted in time-dispersive channels, depends on the frequency-domain channel transfer function (Bohge *et al.*, 2007, Keller and Hanzo, 2000b).

Transmission techniques which do not adapt the transmission parameters to the fading channel require a fixed link margin or coding to maintain acceptable performance under

deep fade conditions. Thus, these systems are effectively designed for the worst-case channel conditions, resulting in an insufficient utilization of the available channel bandwidth. Conversely, if the channel fade level is known at the transmitter, Shannon capacity is achieved by matching transmission parameters to time-varying channel: the signal transmitted to and by a particular station can be modified to take into account the signal quality variation.

Usually, wireless systems adopt power control as the preferred method for link adaptation. In a system with power control, the power of the transmitted signal is tuned in order to maintain the quality of the received signal at each individual subcarrier. Therefore, the transmit power will typically be low when a user is close to the base station (BS) and it will increase with the distance from the BS.

Power control is based on the water filling theorem: given a certain power budget, more transmit power is applied to frequencies experiencing lower attenuation. Thus, given the transfer function, the optimal power distribution is similar to inverting the transfer function and pouring a liquid (i.e. power) into the shape.

Although the use of just power control can improve the system performance in terms of the Bit Error Rate (BER), the total channel capacity is not used efficiently at any transmission time, if the modulation scheme is fixed. To overcome this drawback, Adaptive Modulation and Coding (AMC) or subcarrier allocation should be considered. In a system with AMC, the power of the transmitted signal is held constant but the modulation and coding orders are changed to match the current received signal quality. Users close to the BS are typically assigned higher-order modulations and higher code rates but the modulation order and/or the code rate usually decrease when their distance from the BS increases (Keller and Hanzo, 2000a).

Furthermore, in a multiuser OFDMA wireless network where the given system resources are shared by several terminals an adaptive subcarrier allocation strategy can significantly increases the system capacity by exploiting the *multiuser diversity*: the channel characteristics for different users are almost mutually independent; more attenuated subcarriers for a user may not result in a deep fade for other users. Subcarrier allocation strategies dynamically assign subcarriers with the best frequency response to the users.

Subcarrier allocation strategies can follow different criteria, such as having a fair data rate distribution among users or to maximize the overall network throughput. A possible subcarrier allocation strategy has been proposed by Rhee and Cioffi (2000) with the aim of obtaining almost equal data rates for all users. With this strategy more resources are allocated to users with bad channel conditions or far away from the BS. As a consequence, the capacity of users with good channel conditions are not fully exploited. Absolute fairness may lead to low bandwidth efficiency. However, throughput maximization is sometimes unfair for those users with bad channel conditions.

Adaptive subcarrier allocation techniques have been addressed, also jointly with other resource-allocation strategies, by Kim *et al.* (2005), Kulkarni *et al.* (2005), Wong *et al.* (1999) and Ermolova and Makarevitch (2007). The adaptive subcarriers and bits assignment scheme presented by Kulkarni *et al.* (2005) has the aim of minimizing the total transmitted power over the entire network while satisfying the data rate requirement of each link. Ermolova and Makarevitch (2007) considered a low-complexity suboptimal power and subcarrier allocation for OFDMA systems, proposing a heuristic noniterative method as an extension of the ordered subcarrier selection algorithm for a single user case to OFDMA systems.

The traffic types and services made by the devices composing a WMAN are strongly specialized and they have to be scheduled respecting transmission time and used bandwidth constraints. In order to provide the compliance of service parameters and QoS, a traffic management model is needed: IEEE 802.16 divides all services in four different groups, distinguished by traffic parameters, bandwidth request and resource-allocation techniques. However, WiMAX does not specify any *uplink* or *downlink* scheduling algorithm.

Recently the scheduling issue of multimedia traffic in wireless network has become a hot topic for the research community. Song and Li (2005) proposed a utility-based function for resource allocation and scheduling for downlink traffic in an OFDM-based communication system by exploiting wireless channel status jointly with packet queue information. Cai *et al.* (2005) proposed a downlink resource management technique for OFDM wireless communication systems, considering different traffic types and by exploiting subcarriers and power allocation. Liu *et al.* (2001) discussed the principles of opportunistic scheduling in resource-sharing wireless communication by focusing on the time varying conditions of the physical channel. Wong *et al.* (1999) devoted particular attention to the resource allocation in OFDMA systems. In particular, a suitable adaptive subcarrier, bit and power allocation algorithm is proposed for the case of a frequency selective wireless channel. Likewise, Ergen *et al.* (2003) proposed a fair scheduling technique that exploits subcarriers and bit allocation for an OFDMA wireless system.

Cicconetti *et al.* (2007), Lee *et al.* (2005) and Niyato and Hossain (2006) investigated the resource management for the case of IEEE 802.16 systems. Cicconetti *et al.* (2007) presented a performance evaluation for the different scheduling services offered in the IEEE 802.16 standard, by focusing on a Frequency Division Duplexing (FDD) system. Niyato and Hossain (2006) performed a queue analysis for IEEE 802.16 networks by considering real-time services and their impact on the highest priority traffic. Finally, Lee *et al.* (2005) investigated the VoIP service in IEEE 802.16 networks by focusing on the uplink and a mobile environment.

7.3.1 System Model and Problem Formulation

The system under consideration, as specified by the IEEE 802.16e standard, exploits the OFDMA among users for allocating the resources.

On the other hand, each user terminal is supposed to have different requirements of bandwidth and bit rate due to the type of traffic to be sent out and the QoS constraints especially in terms of priority (e.g. video-monitoring sensor networks or alarm delivery). Finally, we assume that the BS and user terminal transmits on each subcarrier with the same power, that is fixed and independent from the total available power and number of allocated subcarriers (Rhee and Cioffi, 2000).

For optimizing the access scheme two main aspects have to be considered: the adaptation of the modulation and coding and the optimization of the scheduling. Both aspects depends on the channel behavior as well as on the QoS requirements of each device in the coverage area.

7.3.1.1 AMC techniques

AMC denotes the possibility of choosing the most suitable modulation and channel coding scheme according to the propagation conditions of the radio link (channel state) known at the transmitting end.

For our purposes we have considered that the channel quality degradation is mainly due to the path loss and multipath fading.

There are mainly two types of AMC technique: maximum throughput AMC, in which the Modulation and Coding Scheme (MCS) is selected to achieve the best overall throughput without any constraint on the data reliability (i.e. bit error probability), and minimum bit error probability AMC, in which, conversely, the main goal is to meet specific data reliability constraints and, hence, the MCS is selected accordingly.

7.3.1.2 Scheduling Strategy

The aim of a scheduling strategy is to perform an optimal allocation of the network resources among the users in order to maximize the overall network throughput and meet the user QoS constraints in terms of minimum bit rate needed, $R^k_{\min}$, and $\bar{P}_{\text{ber}}$. From above, it follows that the objective is to search for the subcarriers allocation matrix $\mathbf{M}$ for which we have:

$$\max_{\mathbf{M}} \sum_{k=0}^{K-1} \sum_{n \in \mathbf{M}_k} r_k(n) \quad \text{such as} \begin{cases} \sum_{n=0}^{N-1} r_k(n) \geq R^k_{\min}, & \text{for all } k, \\ \sum_{k=0}^{K-1} \delta\left[r_k(n)\right] \leq 1, & \text{for all } n, \\ P_{\text{ber}} \leq \bar{P}_{\text{ber}}, \end{cases} \tag{7.1}$$

where $r_k(n)$ is the bit rate achieved by user k on subcarrier n, $\delta[\cdot]$ is the Kronecker delta function, $\mathbf{M}_k$ is the allocation matrix for user k, K is the total number of users and N the total number of subcarriers. Note that $\mathbf{M}$ can be considered as a time-frequency grid with the x-axis and y-axis formed, respectively, by the number of OFDM symbols contained in a frame and all of the subcarriers.

7.4 Secure Communications Approaches

Security services are essential for any modern network, whether they are general purpose networks, such as a network for access delivery or specific purpose-driven networks. In general, security services such as *authentication*, *confidentiality*, *access control*, *integrity* and *availability*, as defined by Stallings (2006) have to be guaranteed in most real-life scenarios. In the context of monitoring of wide areas, the security of the overall system depends on the security features of each component and from their interaction. In this section we briefly review the security features of the building blocks of the monitoring network.

The most delicate component of the system is surely the WSN, for the hardware limitations and for the specific requirements it presents. In general, security in WSN is an underestimated feature, meaning that the stringent hardware requirements force the designers to give more attention to other details. Still, the application that a WSN can be targeted to are often critical and some security services should be guaranteed. We give three practical example scenarios.

- In a surveillance network an intruder must be unable to alter the flow of information toward the gateway, or pollute the gateway with fake messages. We can imagine an

attacker that wants to access a restricted area using a laptop to flood the nodes, or to hijack routing protocols in order to prevent the gateway from receiving alarms.

- In a WSN for home automation it is imperative to guarantee some form of access control in order to avoid an attacker from taking control of the environment.
- In a body network the parameters that are monitored are private and should not be disclosed. If the parameters are processed automatically to control health equipment authentication and access control is, again, fundamental.

The hardware used for WSN is unable, in most cases, to perform the computation necessary to use public/private key schemes which is a great limitation since most of the modern security protocols are based on such algorithms. This makes the WSN a stand-alone network that must be interfaced with the rest of the system, but cannot be easily integrated.

Another important issue is the degree of distribution that a WSN implements. In general, security schemes are easier to implement when there is a strict hierarchy between the components of a network. If the WSN presents a star topology, with a single gateway always reachable by all of the nodes, the security associations between the nodes and the gateway can be easily pre-loaded. Otherwise if the WSN is a multi-hop mesh network with an unpredictable (and even varying) topology the security association between a couple of nodes that share the same link must be automatically negotiated using some pre-shared credentials, which introduces scalability problems.

Lastly, WSN are generally unattended, nodes can be stolen, their keys can be compromised and even the software can be reprogrammed. Large-area WSNs should resist the presence of a certain number of compromised nodes.

A completely different situation can be found in the transport WiMAX network. First of all, most of the time WiMAX networks use a centralized model which helps the creation of a security hierarchy, then WiMAX standards mandate that the equipment must be capable of performing computations needed for public/private key cryptography; lastly, robust security protocols can be used. Nevertheless some severe vulnerabilities have been found in IEEE 802.16d, in part fixed in the later IEEE 802.16e.

The security scheme used in WiMAX is distinct for the so-called Point-to-Multipoint (PMP) mode, in which a BS serves various clients, and the *mesh* mode in which a certain number of peers form a distributed flat network. In the first case the authentication of a IEEE 802.16d network is based on an original protocol designed for WiMAX which makes use of RSA certificates. The standard mandates that each network client should be in possession of a factory installed certificate that bounds the MAC address of the device to an RSA key, and this key is used to perform authentication to the BS. With a packet exchange defined in the standard, two fresh symmetric keys are generated during authentication, the so-called *AK* and *TEK*, where the first is used as a proof to perform periodical re-authentications the second is used for encrypting and authenticating data. The introduction of mandatory RSA certificates and hardware capable of performing public key cryptography is a new feature that distinguishes WiMAX from previous standards. With such feature it should be possible to prevent an attacker from stealing the MAC address of another client in order to access the network. In a WiFi network, for example, MAC-based access lists are widely used but they are much more insecure then certificate-based authorization. Nevertheless, the overall security scheme of IEEE 802.16d has been proven to be insecure (Maccari *et al.*, 2007). Briefly, some of the defects that it presents are as follows.

- Authentication is always mono-directional. As happened in IEEE 802.11 networks with the Wired Equivalent Privacy (WEP) security standard the BS never authenticates itself with the subscriber stations. This gives to an attacker the possibility of creating a *rogue* network in which the clients might authenticate.

- There is no message authentication code in the frames, even after that the authentication has been accomplished and keys have been derived. This exposes the standard to reply attacks.

- The use of the Data Encryption Standard (DES) encryption algorithm (Cipher Block Chaining (CBC) mode) is unsafe if not associated with a message authentication code. The attacker might be able to interfere with the decryption of frames into the client nodes.

- Some sensitive information is sent from and to the BS without authentication, so that an attacker could inject false data. For instance, the frames that the client stations use to request the activation of new QoS profiles are not authenticated, so that an attacker can send spoof requests pretending to be any other client.

- There is no means of performing certificate management on the BS. Certificate and access lists are hard-coded into the BS and no reference has been made to the use of Authentication, Authorization and Accounting (AAA) protocols such as RADIUS (Remote Authentication Dial-In User Service). This makes the security features much harder to use.

- Authentication is based only on the device certificate, there is no user authentication.

The experiences conducted with WiFi networks highlight that when the price of the devices lowers, the network security is much more stressed because any commercial device can be used by an attacker. At present, WiMAX devices are still high-end devices, but when they reach a higher diffusion legacy, 802.16d devices will be much more difficult to defend.

In the 802.16e revision the 802.16 working group have addressed some of these problems. First of all the legacy authentication scheme, PKMv1, has been substituted by a modular and more modern PKMv2, based on EAP (Extensible Authentication Protocol) and RADIUS. Such a change is of great importance because it introduces a modular approach to authentication, that is not performed on the BS but is relayed to a separate authentication server. This allows a fully centralized user management that starts with a bi-directional authentication and continues with authorization (assignment of user profiles and capabilities based on the pair *user–device*) and accounting (profiling of user activities). EAP allows any kind of authentication to be performed, based on certificates, passwords or other credentials. Encryption has been upgraded to more robust algorithms and MAC has been added to authenticated frames. Still, some management frames have been left unauthenticated, which exposes IEEE 802.16e networks to the problems described before.

To understand the importance of this upgrade, note that the WiMAX Forum, which is able to give WiMAX certifications in the stage two version 1.0.0 specification, do not allow the certification of PKMv1 devices.

The introduction of a centralized authentication server recalls the model used for IEEE 802.11i, and detailed in IEEE 802.1X. It eases the management of a wide area network but

also introduces great delays in the authentication operations, since every time a node has to be re-authenticated it needs to complete the authentication not with its own BS (with which it is connected with a wireless link) but with a server that can be several hops away, introducing a delay that can be even several seconds long.

A more complex situation is present for mesh networks. In a mesh WiMAX network as defined in the standard the authentication of nodes is performed exactly as in the PMP mode, but the derived AK key is the same for every node in the network. It is not clear how this key should be refreshed, which introduces more security problems.

In a mixed WSN–WiMAX scenario, the security of the overall system depends on the security of each component of the network, but also from the interfaces chosen to make them interact. In particular, the information should be secured along the entire chain of transmission, and the sources of information should be certified from bottom to top. This implies the creation of opportune Interworking Functions (IWFs) that match the security features of each single component respecting user attributes.

As an example, imagine a multi-hop WSN where each node has a security association with all of its closest one-hop neighbors. Data is collected from each single node, transmitted over a wireless link to a neighbor and conveyed over a multi-hop path to the gateway. Each link is secured by a key negotiated with an algorithm as in Fantacci *et al.* (2008) or Chan *et al.* (2003) and intermediate nodes can perform data fusion before the frames reach the gateway. The gateway has a WiMAX link that can end directly in the BS, or it can be part of a mesh network of BSs connected to Internet. Information can be gathered also by mobile data sinks, that walk across the WSN and collect the measures directly from the nodes of the WSN.

Given this generic scenario, let us analyze a possible organization of the network security scheme.

- Information is sensed by a node, and transported over a wireless link that is secured by a shared key (data is ciphered and authenticated). If the link is direct to the gateway, the gateway will map the data to a single node, if there is a multi-hop path to the gateway and each intermediate node can perform data fusion, there is no strict association between a single node and the information that reach the gateway.

- From the gateway, the link to the BS is secured by a WiMAX wireless connection that is authenticated with a RSA certificate or any other EAP method. The gateway will possibly aggregate and elaborate the sensed data, so that the data will be seen by the backbone as coming from the gateway itself.

- On the WiMAX backbone data will be moved using the mesh configuration, so authentication will be based on a single AK key.

- The WiMAX network will end with an IP gateway, connected to the Internet: from this gateway to a control center a Virtual Private Network (VPN) can be used to secure traffic.

Basically in this scheme each level of the network is masquerading as a lower layer, as represented in Figure 7.2. This configuration is easy to deploy because masquerading avoids the problem of defining low-level IWFs between the different protocol stacks.

Now let us imagine that the control center receives an alert that is later shown to be false, so that there is suspicion that any of the link of the chain has been compromised. The

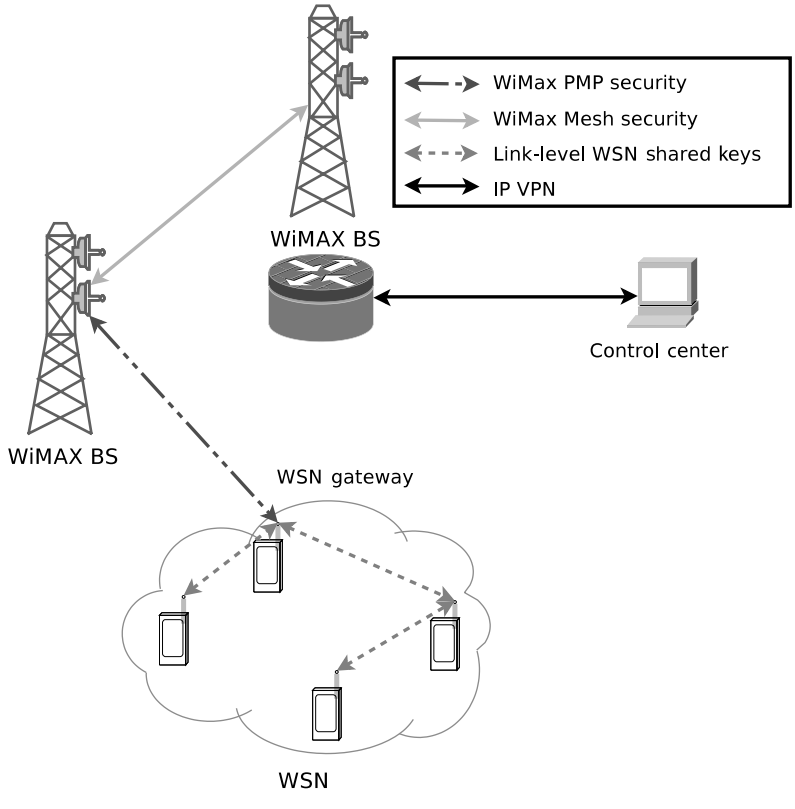

Figure 7.2 Security architecture based on link-layer protocols.

compromised link could be the single sensor node that generated the false information, but it could be also any node on the path to the gateway that performed data fusion. Alternatively it could be coming from a compromised gateway, or it could even have been injected over a compromised WiMAX link.

Another difficult issue to resolve is key revocation, when one of the mobile sinks is stolen. Mobile sinks draw data directly from the sensor nodes, so they need a key shared with each of them. It is not an easy task to reprogram every node in order to invalidate that key. We see that a layered approach has disadvantages under a security and management point of view. Now let us imagine a completely opposite scenario.

- Each sensor node is in possession of a shared key with a unique authentication server, for the whole network. Each time a node wants to create a link with one of its neighbors, it will communicate with the authentication server and ask for a fresh shared key. Communications with the authentication server must pass through the sensor technology, WiMAX links and Internet with proper encapsulation. In this way the WSN mesh is formed.

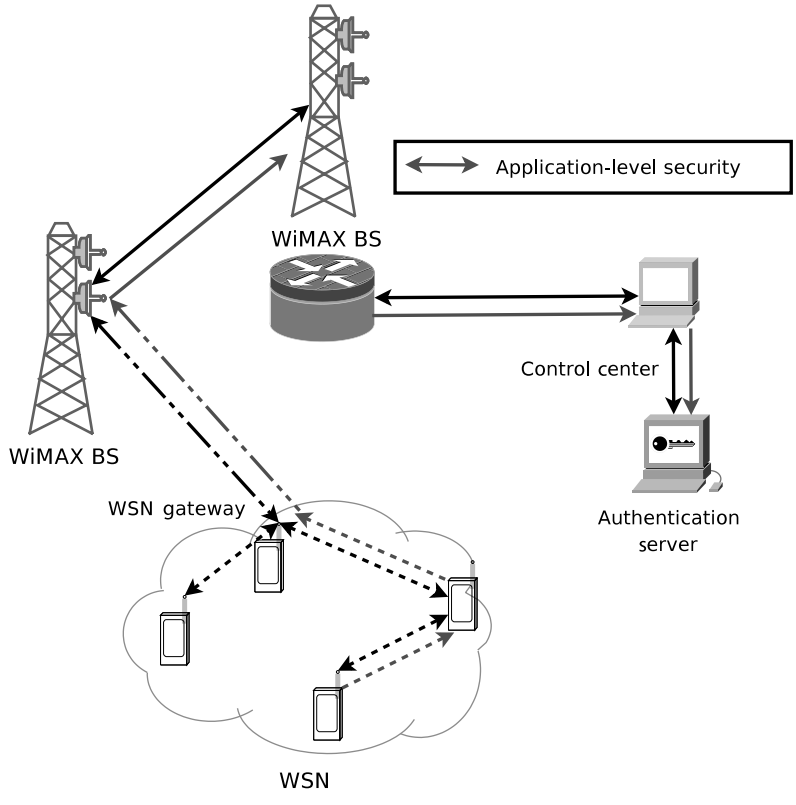

Figure 7.3 Security architecture based on end-to-end protocols.

- When the node wants to send information it will sent a frame ciphered and authenticated with its key, that will be encapsulated in the WiMAX link.

- The control center receives data that are authenticated directly by the single nodes.

We see that in such a configuration as depicted in Figure 7.3, there is an end-to-end authentication, so that a misbehaving sensor node can be recognized in the control center. Moreover, since links are dynamically created with the help of an authentication server, a stolen node can be easily excluded by the network revoking its keys and credentials from the server. On the other side such a configuration introduces new difficulties in managing the whole network. Since data is authenticated and ciphered, no fusion can be made along the path, and information can be lost on the way (for instance, the gateway in the field might know information useful for data fusion, such as the position of the sensors, which will not be available in the control center). Then, for each link that has to be created, a multi-hop, multi-technology handshake must be fulfilled. Lastly, specific encapsulation must be defined for every network bridge.

Acknowledgements

This work is partially supported by MIUR-FIRB Integrated System for Emergency (InSyEme) project under the grant RBIP063BPH and by the Italian National Project Wireless multiplatfOrm mimo active access netwoRks for QoS-demanding muLtimedia Delivery (WORLD), under grant number 2007R989S.

References

AgroSense (2007–2010) Wireless sensor networks and remote sensing – foundation of a modern agricultural infrastructure in the region, http://www.agrosense.org/.

Akyildiz, I., Su, W., Sankarasubramanian, Y. and Cayirci, E. (2001) Wireless sensor networks: a survey. *Computer Networks*, **38**, 393–422.

Bohge, M., Gross, J., Wolisz, A. and Mayer, M. (2007) Dynamic resource allocation in OFDM systems: An overview of cross-layer optimization principles and techniques. *IEEE Network*, **21**(1), 53–59.

Cai, J., Shen, X. and Mark, J.W. (2005) Downlink resource management for packet transmission in OFDM wireless communication systems. *IEEE Transactions on Wireless Communications*, **4**(4), 1688–1703.

Chan, H., Perrig, A. and Song, D. (2003) Random key predistribution schemes for sensor networks. *Proceedings of 2003 Symposium on Security and Privacy*, pp. 197–213.

Chiti, F. and Fantacci, R. (2006) Wireless sensor network paradigm: overview on communication protocols design and application to practical scenarios. *EURASIP Newsletter* **17**(4), 6–27.

Cicconetti, C., Erta, A., Lenzini, L. and Mingozzi, E. (2007) Performance evaluation of the IEEE 802.16 MAC for QoS support. *IEEE Transactions on Mobile Computing*, **6**(1), 26–38.

DustBot (2007–2009) Networked and cooperating robots for urban hygiene, http://www.dustbot.org/.

Ergen, M., Coleri, S. and Varaiya, P. (2003) QoS aware adaptive resource allocation techniques for fair scheduling in OFDMA based broadband wireless access systems. *IEEE Transactions on Broadcasting*, **49**(4), 362–370.

Ermolova, N.Y. and Makarevitch, B. (2007) Low complexity adaptive power and subcarrier allocation for OFDMA. *IEEE Transactions on Wireless Communications*, **6**(2), 433–437.

Fantacci, R., Chiti, F. and Maccari, L. (2008) Fast distributed bi-directional authentication for wireless sensor networks. *Journal on Security and Communication Networks*, **1**(1), 17–24.

GoodFood (2004–2006), http://www.goodfood-project.org/.

Ilyas, M. and Mahgoub, I. (2005) *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. CRC Press, Boca Raton, FL.

InSyEme FIMFR (2007–2010) Integrated System for Emergency, http://www.unifi.it/insyeme/.

Keller, T. and Hanzo, L. (2000a) Adaptive modulation techniques for duplex OFDM transmission. *IEEE Transactions on Vehicular Technology*, **49**(5), 1893–1906.

Keller, T. and Hanzo, L. (2000b) Adaptive multicarrier modulation: a convenient framework for time-frequency processing in wireless communications. *Proceedings of the IEEE*, **88**(5), 611–640.

Kim, K., Han, Y. and Kim, S.L. (2005) Joint subcarrier and power allocation in uplink OFDMA systems. *IEEE Communications Letters*, **9**(6), 526–528.

Kulkarni, G., Adlakha, S. and Srivastava, M. (2005) Subcarrier allocation and bit loading algorithms for OFDMA-based wireless networks. *IEEE Transactions on Mobile Computing*, **4**(6), 652–662.

Lee, H., Kwon, T. and Cho, D.H. (2005) An enhanced uplink scheduling algorithm based on voice activity for VoIP services in IEEE 802.16d/e system. *IEEE Communications Letters*, **9**(8), 691–694.

Liu, X., Chong, E.K.P. and Shroff, N.B. (2001) Opportunistic transmission scheduling with resource-sharing constraints in wireless networks. *IEEE Journal on Selected Areas in Communications*, **19**(10), 2053–2064.

Maccari, L., Paoli, M. and Fantacci, R. (2007) Security analysis of IEEE 802.16. *Proceedings of the 2007 IEEE International Conference on Communications.*

Niyato, D. and Hossain, E. (2006) Queue-aware uplink bandwidth allocation and rate control for polling service in IEEE 802.16 broadband wireless networks. *IEEE Transactions on Mobile Computing*, **5**(6), 668–679.

Rhee, W. and Cioffi, J.M. (2000) Increase in capacity of multiuser OFDM system using dynamic subchannel allocation. *Proceedings of IEEE VTC 2000-Spring*, vol. 2, Tokyo, Japan, pp. 1085–1089.

Song, G. and Li, Y.G. (2005) Utility-based resource allocation and scheduling in OFDM-based wireless broadband networks. *IEEE Communications Magazine*, **43**(12), 127–134.

Stallings, W. (2006) *Cryptography and Network Security*. Prentice Hall, Englewood Cliffs, NJ.

IEEE (2005) Amendment to IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands. *IEEE Standard 802.16e-2005*.

IEEE (2004) IEEE Standard for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems. *IEEE Standard 802.16-2004.*

van Nee, R. and Prasad, R. (2000) *OFDM for Wireless Multimedia Communications*. Artech House.

Wong, C.Y., Cheng, R.S., Letaief, K.B. and Murch, R.D. (1999) Multiuser OFDM with adaptive subcarrier, bit, and power allocation. *IEEE Journal on Selected Areas in Communications*, **17**(10), 1747–1758.

WP122 (2008) Report on experimental capabilities of the integrated test bed. *Technical Report FP6-IST-4-027738-NoE, 'CRUISE'.*