Telecommun Syst
DOI 10.1007/s11235-009-9235-0

The future of security in Wireless Multimedia Sensor Networks

A position paper

Manel Guerrero-Zapata · Ruken Zilan · José M. Barceló-Ordinas · Kemal Bicakci · Bulent Tavli

Abstract This is a position paper on our views on security aspects of Wireless Multimedia Sensor Networks (Secure WMSNs). It is meant to serve as a brief survey. But, more importantly, it gives a perspective on how we foresee the future of this research area, its main challenges, and its future trends. We believe that this paper will spur new discussions and research ideas among the researchers from both the industry and the academic world.

Keywords Security · Wireless Multimedia Sensor Networks · WMSN

This work has been supported by Spanish Ministry of Science and Technology under grant TSI2007-66869-C02-01 and by NoE EuroFGI VI FP.

M. Guerrero-Zapata (✉) · R. Zilan · J.M. Barceló-Ordinas
Computer Architecture Department (DAC), Technical University of Catalonia (UPC), Jordi Girona 1-3, Campus Nord, Office C6-123, 08034 Barcelona, Spain
e-mail: guerrero@ac.upc.edu

R. Zilan
e-mail: rzilan@ac.upc.edu

J.M. Barceló-Ordinas
e-mail: joseb@ac.upc.edu

K. Bicakci
Electrical and Electronics Engineering Department, TOBB University of Economics and Technology, Sogutozu 43, Office Z69, Sogutozu, 06560 Ankara, Turkey
e-mail: bicakci@etu.edu.tr

B. Tavli
Computer Engineering Department, TOBB University of Economics and Technology, Sogutozu 43, Office 169, Sogutozu, 06560 Ankara, Turkey
e-mail: btavli@etu.edu.tr

Published online: 03 December 2009

1 Introduction

Wireless Multimedia Sensor Networks (WMSN) are gaining research interest due to the availability of low-cost cameras and CMOS image sensors, also due to their broad application opportunities [1]. WMSN applications range from surveillance and monitoring to industrial control, or personal health care. These applications incorporate transmission of different kinds of data, such as *still images*, *multimedia streaming* and *audio*.

Still images are used usually in the transmission of event triggered observations during short periods of time, while multimedia streaming requires the transmission of large amounts of real time traffic over longer periods of time.

The resources needed, in general, by multimedia traffic in terms of buffering, bandwidth, battery consumption, and processing are higher than the resources required in Wireless Scalar Sensor Networks (WSSNs). Multimedia data requires sensor platforms that provide higher data rates. Predictive encoding techniques (e.g. motion estimation) need buffering and processing capabilities not present in current sensor network platforms. Novel coding techniques (e.g., distributed source coding [2]) are proposed to build less complex coders (e.g. sensors) at the cost of more complex decoders (e.g. sinks). But, on the other hand, the amount of visual data to be transmitted is reduced if in-network processing is performed at the source. In-node processing techniques manipulate data in such a way that only a small amount of metadata describing the object of interest is transmitted (e.g., background subtraction or edge detection) at the cost of increased computation. Thus, power consumption due to computation will be a factor to be considered in WMSN.

The lessons learned from protocol design for Mobile Ad hoc Networks (MANET) and for WSSN leads us to the conclusion that security is critical and should be taken into ac-

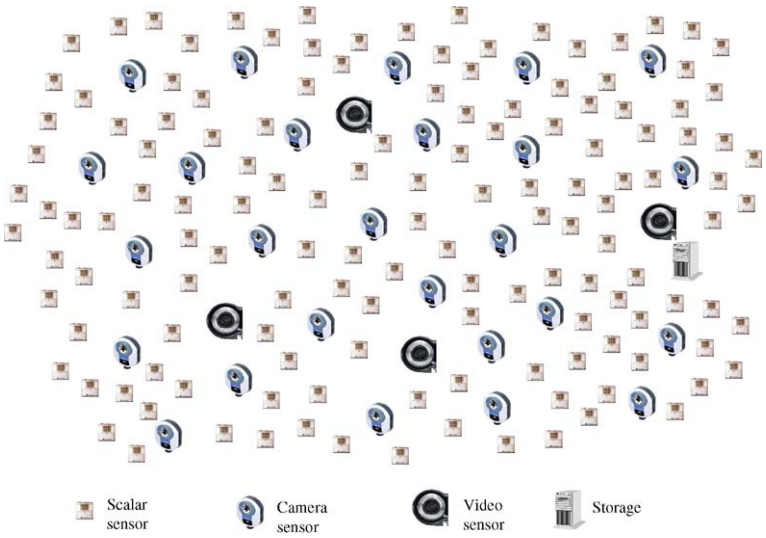

Fig. 1 Multi-tier architecture

count from the start. WMSN research community might be tempted to hastily assemble protocols without properly provisioned security features. Nevertheless, experience shows us that when, later, security measures are tried to be retrofitted to those protocols, most of the time it will not be feasible and the original design decisions will not be valid ones anymore.

This paper provides a survey and analysis of the different security issues that will have to be taken into account in the design of WMSN platforms and protocols. While other papers give a general view of WMSN [1], they do not analyze the security aspects of WMSNs deeply.

The rest of this paper is organized as follows: Sect. 2 explains current technologies and architectures in WMSN, discusses their limitations and gives a state of the art on some current protocol proposals. Section 3 presents a summary of the related work on WSSN and WMSN security. We present the differences and similarities of WSSN and WMSN from a security point of view in Sect. 4. Section 5 analyzes future trends and challenges of the security related aspects of WMSN and conclusions of this study are drawn in Sect. 6.

2 Current technologies in WMSN

The primary function of a Wireless Sensor Network (WSN) is to collect and disseminate critical data that characterize the physical phenomena within the target area. Depending on the application scenario WSN can be categorized into two main streams: WSSN and WMSN. In WSSN, data harvested from the environment is of scalar nature and obtained from various integrated or external sensors such as humidity, temperature, light, accelerometer, pressure, magnetometer, Infrared (IR), seismic, and acoustic sensors. In WMSN, data harvested from the target area is more complex such as streaming video. Hence the main sensor in a WMSN is the imager. Handling visual data puts severe constraints on a sensor network. Collection, processing, and dissemination of visual data is a processing intensive and high bandwidth demanding operation.

Data extraction and processing are considered to be low energy dissipation tasks in WSSNs. Therefore, energy dissipation in scalar sensor nodes is dominated by data transport (communication) energy dissipation. In fact, energy dissipation characteristics of most WSSN platforms confirms this assumption. For example, communication energy dissipation constitutes 91% and 62% of the total energy dissipation in Telos and MicaZ scalar sensor nodes, respectively [3]. Unlike in scalar sensor nodes, energy dissipation in multimedia sensor nodes is dominated by the computation energy rather than the communication energy. For example, communication energy dissipation constitutes only 22% of the total energy dissipation for MicrelEye [4] multimedia sensor node.

Akyildiz et al. [1], propose three general reference architectures for WMSN. The first reference model is a single-tier flat homogeneous (multi-hop) camera sensor network where the sink is a wireless gateway connected to a centralized storage hub. In this model the processing is distributed among the camera sensors. The second reference model is a single-tiered clustered network with heterogeneous sensors. Camera, audio and scalar sensors relay data to a cluster-head able to perform intensive data processing and the cluster-head is connected to a gateway as in the first model. The third model is a multi-tier architecture with heterogeneous sensors. In the first tier, scalar sensors perform simple tasks, like motion detection. A second tier of camera sensors perform more complicated tasks such as object detection or object recognition. At the end point, high end video sensors are connected to wireless gateways (see Fig. 1).

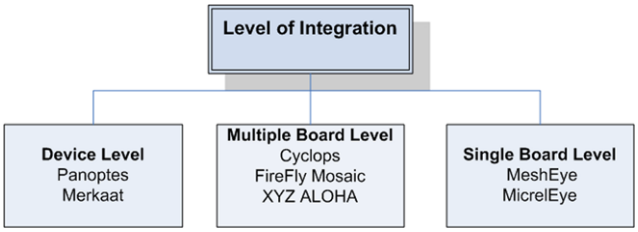

Fig. 2 WMSN platforms

As it happens with WSSN, the application will determine the reference WMSN architecture. For example, SensEye [5], is a multi-tier network of wireless sensor nodes and camera sensors that have different capabilities across tiers in a surveillance application. SensEye follows the third reference model, where it performs three tasks: object detection, recognition and tracking. Each task is performed by a different tier; the lower tier (comprising low-fidelity camera sensors) performs object detection. The second tier (comprising Stargate nodes with Webcams) performs object recognition. The third tier (composed by PTZ cameras) performs object tracking. Figure 2 shows some of the current proposed WMSN platforms and prototypes classified according to the hardware level of integration [6].

In order to reduce the amount of visual data to be sent, in-network processing techniques (e.g., object recognition and object tracking) together with image compression and coding techniques gain importance. Instead of sending the whole frames, only the detected objects of interest are sent by the sensor [3]. However, these algorithms require powerful processors and large memories, which are strong assumptions for WMSN platforms. Nevertheless, energy dissipation and bandwidth constraints imposed by WMSNs necessitate the design, development and implementation of efficient vision algorithms that can be realized by embedded WMSN platforms [7–9]. Novel coding techniques are proposed such as Distributed Source Coding (DSC) [2] that exploits Slepian-Wolf and Wyner-Ziv theorems suggesting that it is possible to compress two statistically dependent signals in a distributed manner resulting in a coding design with low complexity encoders and high complexity decoders.

There has been some research activity in the field of WSN with QoS, but almost exclusively considering scalar sensors subject to QoS metrics [10, 11]. Only a few studies in the field of protocols and algorithms specifically considered WMSNs. Two Phase geographical Greedy Forwarding (TPGF) [12] is a routing protocol for exploring one or multiple optimized hole-bypassing transmission paths. MultiPriority MultiPath Selection (MPMPS) [13] is a scheme for transport layer to choose disjoint paths maximizing streaming data transmissions and guaranteeing the end-to-end transmission delay. Ant-based Service Aware Routing (ASAR) [14] chooses paths according to QoS requirements and defines three types of services: Event-driven services, data query-driven services and stream query-driven services. However, these studies do not take into account the intrinsic characteristics of multimedia traffic (e.g., burstiness).

Although the majority of the research in WMSNs follow strict layerist architectures there are some WMSN specific cross-layer proposals. For example, Video Sensor Network Module (VSN-module [15]) is a cross-layer communication protocol providing QoS support. VSN-module uses a TDMA scheme for medium access based on RR-ALOHA. On top of a geographical protocol schedule packets based on hop-by-hop path reservations are used. These reservations use a cross-layer decision function that takes into account energy constrains, error control, number of neighbors (connectivity constraints), and buffer capabilities (local congestion control). Nodes generate video flows according to video frame rates, resolution and color depth.

In summary, we can say that there are not many studies and research on WMSN protocols, algorithms, and architectures. The main QoS research proposals are focused on providing QoS to WMSNs without considering the intrinsic nature of multimedia content. We expect an intensified research effort in this area in the following years and, therefore, security issues should also have to be taken into account.

3 Related work on security in WSSN and WMSN

In this section, we provide an overview of literature on security in WSSN and WMSN.

3.1 Related work on security in WSSN

In the context of WSSN, security means to protect sensor data against unauthorized access and modification and to ensure the availability of network communication and services in spite of malicious activities. If collected data is private and sensitive such as user location information, then privacy issues are also of concern. Below, we review important issues and proposed solutions in the literature concerning WSSN security and privacy.

The classical means to ensure integrity and confidentiality of data is to use cryptographic algorithms. In all modern crypto primitives, the security more or less depends on the security of the cryptographic keys hence the distribution and management of keys has a vital importance. As we know, public key cryptography simplifies key management by allowing secure communication by distributing n public key-private key pairs in a network having n nodes whereas the same problem can be solved by distributing $n * (n-1) \approx n^2$ keys with symmetric key cryptography (each one of the total of n nodes are pre-installed with $n-1$ keys and total number of keys generated is $n^2/2$). Besides, key revocation,

which is generally needed to avoid node-capture and sybil (multiple-identity) attacks in WSSN, is more complex in a symmetric-key setting. Although symmetric key cryptography has such problems, previous studies revisit and make in depth investigations on symmetric key management in the context of WSSN [16–20]. The main research problem they have targeted is to reduce the number of symmetric keys distributed in sensor nodes to overcome storage limitations of sensor nodes. Here, one challenge is to keep the probability of establishing a common secret key for a communication channel above a certain level. There are other challenges such as resilience to node compromise, key revocation, etc. A nice survey of key distribution mechanisms in WSN was written by Camtepe and Yener [21]. In this survey, several classifications and evaluation of solutions for different metrics are provided for those who can easily be confused by so many key distribution alternatives in literature.

The reason why symmetric key management is an issue in a WSSN setting is obvious. The other alternative public key cryptography was considered to be too expensive for resource-limited low-end sensor nodes. While this argument has a merit in some WSSN application scenarios, it is too restrictive to say that public key cryptography is not viable in all sensor network deployments (remember that as usual it is sufficient to use public key cryptography only for establishing a common secret key, then subsequent communication will be secured by symmetric key solutions). To justify this counter-argument, there is a significant body of previous research proposing efficient implementations of public key cryptography in sensor networks. Back in 2004, it was claimed that public key cryptography is feasible for WSSN [22]. The claim was validated by implementing two different public key algorithms in hardware; Rabin's scheme and NtruEncrypt scheme. The NtruEncrypt implementation is highly energy-efficient and consumes less than 20 μW power. There are other early studies showing the viability of implementing more popular public key algorithms (e.g. elliptic curve cryptography (ECC) in hardware [23], RSA algorithm in software [24] and ECC in software [25]).

Memory and processing limitations of sensor nodes may be a concern for choosing the most appropriate security design for a WSSN. However, having a limited amount of battery power and the impracticality of changing batteries in most application scenarios, makes energy-efficiency the most important design criteria.

This is a concern not only for the security aspects, but for almost every aspect of network protocol design. Several papers have addressed the issue of energy efficiency in WSSN security. There is an implementation of ECC and RSA in software on a 8-bit microcontroller platform and the measurements indicate that public key cryptography is viable even in very constrained environments [26]. One other finding was that ECC is more energy efficient than RSA because of shorter signature sizes and, thus, less communication overhead. These results were also validated by [27] which states that the influence of public key cryptography on the sensor node lifetime is not significant.

Although we have addressed the issue of using public-key cryptography in WSSNs in the above paragraphs, it will be appropriate to add a few more words on the implementation of one specific type of public-key cryptography that is ID-based cryptography due to the importance and extra capabilities of this recently emerged alternative. ID-based cryptography can be considered as one additional step after the invention of public key cryptography to further ease the key management problem. The basic idea is to devise a scheme in which any bit string can be a public key. By this way in a WSSN scenario node IDs can be employed as public keys and costs associated with validating public keys is avoided [28]. Although, some initial implementation efforts were carried out [29], we believe that there is still room for improvement (i.e. recent results show that pairing computation which is needed for identity-based encryption takes 5.5 s in a 8-bit microcontroller platform [29]).

The typical traffic pattern in a WSSN is either from a sensor node to the base station (sink) possible using other nodes as relays (multihop communication) or from the base station to sensor nodes. In the later, for efficiency reasons broadcasting of a single packet originating from the base station to all sensor nodes is preferred over unicast one-to-one communication. Authenticating the source of the broadcast packets is simple using one of the public key digital signature schemes, however, once we choose symmetric key methods for efficiency reasons, then we require more delicate designs such as Tesla [30] and its variants (micro Tesla [31] and multi-level micro Tesla [32]). Tesla depends on the loose time synchronization between sender and receivers and uses delayed release of keys by the sender. This implies that sensor nodes should exchange messages and use an important amount of the already scarce bandwidth and memory for synchronization [22]. In addition, built on top of message authentication codes which require very small computational power [33], Tesla cannot offer all the functionalities of digital signatures. If a digital signature solution that does not use public key crypto primitives is needed for WSSN, then there are not many alternatives other than several variants of one-time signature schemes [34].

Revocation of cryptographic keys is needed in a WSSN since, when a node is compromised, so are the keys that it was storing. Several studies evaluate different physical attacks against sensor node hardware and propose countermeasures [35]. Standard precautions for protecting nodes from unauthorized access may complicate attacker's job but revocation of compromised keys is still needed against more sophisticated attacks. The fact that sensor nodes usually cannot be physically protected and the difficulty and cost of

employing tamper-resistance hardware not only makes revocation a more serious problem in WSSN but it also may necessitate major changes in the security architecture. This is because the lack of timely revocation of those stolen keys may lead to false data insertion as well as unauthorized data access but the simple solution of broadcasting authentic revocation messages might be too prohibitive for large sensor networks. One-time sensor is a novel concept and a radical change in the network architecture that can eliminate the need for revocation by pre-installing each sensor only with a one-time cryptographic token [36].

Security is an issue for basic protocols common to all networking technology but which are tailored to satisfy WSSN requirements (e.g. MAC layer [37], routing [38], network synchronization [39]) as well as for more specific protocols and services useful in a given WSSN application (e.g. data aggregation [40], localization [41]). We will address some of these issues for WMSN in Sect. 5.

Besides providing security features such as confidentiality and message integrity, a WSSN should continue its function and keep serving under the threat of Denial of Service (DoS) attacks. An early introduction of DoS attacks and countermeasures in WSSN was written by Wood and Stankovic [42]. Generally speaking, we can say that implementing a DoS-resilient network is very challenging if not impossible. Sensor networks in particular have additional vulnerabilities since they can be physically jammed due to their wireless nature and solutions such as spread-spectrum can only complicate and increase the cost of the jammer. Attackers who are interested in DoS attacks which require less power should proceed to upper layers and they will receive a warm welcome with lots of DoS opportunities there.

There are also privacy aspects of WSSNs. Privacy is a problem with social and technological aspects and usually addressed through privacy policies. The technical challenge is to integrate well-established privacy-enhancing mechanisms into WSSN applications. Privacy risks of sensor networks was explored in [43]. One noteworthy conclusion the authors draw is that protocols defending against traffic analysis bring substantial overheads and due to low energy budget of sensor nodes it is difficult to protect user privacy using the current WSSN technology. We will overview the previous work on traffic analysis in Sect. 5.3.

Security in WSSN is currently a hot topic in academic research and so many bright ideas have emerged in recent years. However there are promising open research directions and we conclude this section by pointing to some of them. First of all, in order to improve security in real WSSN deployments, the availability of portable, fully-functional and user-friendly tools are crucial for practitioners. It is not reasonable to expect implementers getting the hassle of porting the security tools to their platforms thus making these tools portable to emerging WSSN platforms which becomes a real and practical challenge. Secondly, it is questionable that from a security point of view today's assumptions for WSSN will be still valid in the future. Future sensor platforms will not only become more resourceful and less expensive but also they will become heterogeneous in terms of their capabilities and functionalities. They will not be managed by a single authority, and will support mobile applications spanning a greater geographical area (for instance in logistics and transportation applications), and will interact with RFIDs, actuator devices, and other pervasive technologies. The complexity and diversity of tomorrow's WSSN applications will bring a continuing overall challenge for security.

3.2 Related work on security in WMSN

Evidence justifies that WMSN security is indeed a very young research field (i.e., a very recent survey on WMSN [44] only cites one prior work on security—that is [45]). According to Kundur et al. [45], so far researchers have focused on the problem of privacy in WMSN. Beside this, there are only a few more prior studies on the issue, mainly considering the privacy.

Czarlinska and Kundur [46] proposed a novel paradigm for securing privacy and confidentiality in a distributed manner. The suggested paradigm is based on the control of dynamical systems and it requires low complexity for the processing and communication. Czarlinska and Kundur [47], studied the detection performance of event-driven WVSNs, by using back transmission to the cluster-head when frames contain event of interest. The decision mechanism is based on either image processing techniques or using support of a scalar sensor, which includes errors due to hostile attacks. Czarlinska et al. [48], presented attacks that affect the data privacy in visual sensor networks and proposed privacy-promoting security solutions established upon a detected-adversary using a game-theoretic analysis and keyless encryption.

Czarlinska and Kundur [49], investigated the event acquisition properties of Wireless Image Sensor Networks, which includes different techniques at the camera nodes to recognize the differences between event and non-event frames in risky environments that are prone to security attacks.

In addition to these studies, other proposed privacy enhancing techniques include converting video information into abstractions [50], removing personally identifying information [51], and masking authorized subjects [52].

Another area that is receiving an increasing interest from the research community is Free Space Optical (FSO) sensors [53]. FSO communications necessities routing through unidirectional links. Although FSO communications are very interesting for WMSNs due to their high bandwidth support, their application in realistic scenarios is challenging. Since they require LoS (Line of Sight communications),

uneven terrain and obstacles found in real-life deployments could reduce the number of links. Weather conditions, such as fog, rain, heavy snow, and the sun; might render a whole network useless.

Since the use of FSO completely changes the nature of the routing protocols, new security solutions are needed. OPSENET is a novel secure routing protocol for FSO WMSN that prevents outsider attacks via lightweight cryptographic mechanisms [45]. In OPSENET, global picture of the network is established at the base station which can be employed as a watchdog. This provides an effective means to identify some of the most devastating insider attacks [45].

Another interesting new concept is distributed visual secret sharing, introduced in [45] in which the images collected by the sensor nodes are used to generate a large number of copies with a large amount of noise and distributed to different nodes of the network. Attackers with only a few copies will not be able to generate the original image. But, the sink will be able to generate it if it receives sufficient number of copies. We discuss this approach in a more detailed manner in Sect. 5.6.

4 Security issues in WSSN and WMSN: is there a difference?

From the security point of view, there is not a strict border between these two types of networks. Therefore, some of the previous security solutions for WSSN discussed in Sect. 3.1 can be easily adapted for WMSN. However, WMSN also has some novel features which stem from the fact that some of the sensor nodes will have video cameras and higher computation capabilities. This brings new security challenges as well as new protection opportunities. Below, we provide two lists summarizing the key points of challenges and opportunities.

Challenges

1. In addition to data delivery modes typically found in WSSN, WMSN should support snapshot and streaming multimedia transmission [44]. Snapshot multimedia means that event-triggered observations are transmitted to the base in a short time period. Snapshot delivery mode is arguably more vulnerable to DoS attacks, because if the snapshot information is blocked, it might not be detected by the sink.
2. Digital streams have properties distinguishing them from regular messages. These properties may necessitate a substantially different security design as discussed in [44].
3. At the beginning of Sect. 3, we stated that privacy issues are of concern in WSSN, if the collected data is private and sensitive. Video, image and audio data are typically more sensitive than scalar data, such as temperature. Hence, privacy enhancing techniques, such as source location, hiding and distributed visual secret-sharing, discussed in the next section, may be crucial for WMSN.
4. Bandwidth demand to carry uncompressed multimedia data is excessive for most scenarios. Compressing data with existing encoders uses complex algorithms and entails high energy consumption, which is not feasible on most power-constrained sensor nodes. For WMSN, reducing the amount of data using multimedia in-network processing techniques (distributed compression, distributed filtering, etc.) is possible. Nevertheless, this requires a different trust model and new security architecture, i.e., all sensor nodes participating in distributed and collaborative processing should be trustworthy.
5. High-speed requirements for carrying multimedia data draw an interest in free-space optical (FSO) communication. There are security aspects of networking issues unique to FSO WMSN [45].

Opportunities

1. Sensor nodes in WMSN should be powerful enough to satisfy the computational and communication demands required to manage multimedia data. From the security point of view, more powerful nodes mean we could have the capability to employ more advanced solutions. In particular, we believe that the use of public key cryptographic solutions is feasible for most WMSN platforms.
2. Sensor nodes (at least an important percentage of the sensor node in a WMSN) will have bigger storage capabilities than sensor nodes in a WSSN. That extra storage capability can be exploited to use security schemes that were not possible in WSSN, e.g., the storage of other nodes' public keys and many session keys, signed information, nodes' reputation statistics, etc.
3. In WMSN applications, especially video sensing capability, brings the opportunity to detect and identify the attacker. Therefore, while specifying the threat model for WMSN, we should take this new capability into account.

5 The future of security in WMSN

Everything seems to indicate that video surveillance and video monitoring will be one of the main applications for WMSN (even the killer application). Furthermore, visual surveillance is an application where the industry (both civilian and military) will be willing to invest. Since the problem of security in WMSN is so complex, the different solutions

are going to be application and environment dependent. In the case of video surveillance and monitoring, most of the time it can be assumed that all the nodes are trusted initially but later on can be compromised. In this scenarios DoS is going to be one of the most common attacks. Other problems like resilience to traffic analysis and compromised nodes are also going to be of the utmost importance.

The following subsections explore in detail future trends and challenges that security in WMSNs will face. It includes a variety of attacks that can be performed against WMSNs (summarized in Table 1).

Table 1 Attacks against WMSN

Eavesdropping
Traffic Analysis:
Sink Location Detection
Event Location Detection
Intrusion:
Intruder Nodes
Compromised Nodes
Denial of Service:
Physical Attacks
Tampering Attacks
Jamming Attacks
Collision Attacks
MAC Protocol Attacks
Routing Protocol Attacks
Transport Layer Protocols

5.1 The return of asymmetric cryptography

We have already mentioned in Sect. 3 that symmetric cryptography has been widely used in wireless sensor networks mainly because it was argued that asymmetric cryptography algorithms required more processing power than what a typical sensor network platform can offer. But, using the continuously developing technology multimedia sensor nodes will be increasingly more powerful in the following years, even for the sake of properly handling the multimedia (which will include video) data [1]. Moreover, in-node processing is going to be necessary in order to minimize bandwidth utilization. Abstractions of the sensed data will be computed inside the node and the node will decide whether the information sensed should be transmitted and whether it should first send as a part of the abstracted data or as a part of the sensed data [54]. Therefore, asymmetric cryptography will be feasible for wireless multimedia sensor nodes. Moreover, it will be the chosen approach (from routing [55, 56] to node authentication) in many cases.

Furthermore, it has been shown and we have already mentioned in Sect. 3 that even nodes with highly constrained computing power limitations can use asymmetric cryptography when efficient asymmetric algorithms are used. With ECC algorithms going to be, probably, the most used ones because of their efficiency and their use of shorter keys [24, 25, 57]. In conclusion, we foresee that even relatively lightweight WMSN nodes will choose asymmetric cryptography as the best approach in most cases. In addition, time synchronization is generally not going to be needed, since it is only required to provide authentication with symmetric cryptography.

5.2 DoS as one of the main challenges

We argue that DoS will be the main attack to be worried about in most of the WMSN scenarios. This is especially important taking into account that one of the main scenarios for WMSN is going to be video surveillance.

One advantage of WMSN nodes is that they are going to be more powerful than scalar nodes, which translates into more computational power for thwarting DoS attacks. Nevertheless, attackers can always bring even more powerful computing resources to perform their attacks.

As discussed in Sect. 3, DoS attacks are a very complex problem, since they can be performed in so many different ways, and against any of the different communication layers [42] (i.e., physical, link, network, transport, and application layers). In addition, protecting only against a subset of them is obviously useless.

In an attempt to detect DoS attacks—including currently unidentified ones—Intrusion Detection System monitors have been designed [58]. These monitors try to find out (i) nodes that are not behaving according to certain parameters that characterize what is considered as normal behavior and (ii) nodes that are performing a well known attack [59]. Unfortunately, it is complicated to design them in such a way that the number of false alarms is low enough and identification of new attacks comes in timely manner [60]. Moreover, there are several important research challenges when they have to be deployed in large scale WMSNs due to scalability issues [61].

In following subsections we will analyze in greater detail some specific types of DoS attacks (namely tampering, jamming, collision, MAC protocol attacks, and routing attacks).

5.2.1 Tampering attacks

It is a well-known fact that trusting tamper resistance is problematic. We will just refer to the main articles in this area [62–64] which show that—no matter how hard you try—tamper resistant devices are routinely tampered by using inexpensive products and tools.

Therefore, probably the best approach is to assume that tamper resistance is going to have limited effectiveness.

Moreover, limiting the scope and the amount of the sensible information -including keys- stored in each sensor is also important.

In the case of networks that use asymmetric cryptography, in every node there only needs to be its own private key and several public keys. So, when one node is compromised and tampered the damage is a more controlled one. This is another point that supports the use of asymmetric cryptography over symmetric cryptography solutions.

5.2.2 *Jamming attacks*

Attacks at the physical layer performed by emitting a radio signal targeted at jamming a particular channel are very difficult to defend from [65, 66].

Currently there are two main approaches. One approach is to simply use another channel other than the one that is being interfered (called channel surfing) [67, 68]. The second approach tries to achieve communication in the presence of the jamming entity by adjusting resources, such as power levels and communication coding, and by prioritizing the messages the nodes send [69].

One of the challenges about jamming attacks is that the network reaction to the attack must be fast [70]. This is because the attack could be performed by a so called "reactive jammer". A reactive jammer is a jammer that only jams the channel when it detects channel activity. In surveillance applications it could be used to block the sink node to prevent it from getting the reports of an ongoing intrusion.

Although spatial retreat has been suggested as a possible solution for certain WSSN [71], it will arguably not make sense for most of the applications for WMSN.

5.2.3 *Collision attacks*

Collision attacks are an intelligent and efficient way of producing the same end result as the jamming attacks. In a collision attack, the attacker only needs to send a byte when it overhears a packet to force the receiver of the packet to discard the whole message which means that the amount of energy to perform such attacks is much lower when compared to jamming attacks. So far, a proposed solution to this attack has been the use of strong error-correcting codes. Nevertheless, for a given encoding, the attacker can just send more bytes than the error correction codes can correct. In addition, error-correcting codes add a processing and communication bandwidth overhead [69].

Therefore, while there are some preliminary results on how to detect and prevent them [72], it is still a challenging research area. We do not foresee generic error correcting codes based solutions as the right way to go. We would rather recommend to explore the detection and avoidance of paths with attackers that perform collision and jamming attacks. Moreover, only in the scenarios where such approaches are not good enough, the use of traffic specific strong error correcting codes is a feasible approach.

5.2.4 *MAC protocol attacks*

Introducing a node in the WMSN that is purposefully not following the MAC protocol rules in order to achieve DoS (e.g., when the network is sensing an event that needs to be reported) can have devastating results. These attacks can be fairly simple ranging from the well known attack of properly selecting back-off intervals [73, 74] (more typical in selfish nodes of ad hoc networks) to the use of RTS/CTS messages. There are already several studies on how to detect some of the possible MAC protocol attacks [75, 76]. But, obviously further research is needed in this area.

We foresee as in the case of collision attacks that creation of a MAC protocol completely resilient to DoS attacks is not going to be feasible. Therefore, one of the ingredients of an integrated solution will be the use of redundant paths [77] (to avoid paths that are detected to be under attack).

The above mentioned attacks are, however, for networks that use IEEE 802.11. We refer readers interested in the topic of DoS attack and countermeasures in IEEE 802.11 wireless network to [78]. It is important to note that IEEE 802.11 is not the only kind of MAC protocol we are going to see in WMSN [79]. There has been a lot of research to use TDMA MAC protocols especially in order to be able to achieve QoS in WSNs [80–82].

In addition, there are some TDMA MAC protocols which assume that nodes know their two-hop neighborhood topology in order to generate the TDMA schedule locally, without requiring information exchange with their neighbors [83]. There are also CSMA/TDMA hybrid MAC protocols for WSNs [84–87].

Nevertheless, there have not been any studies on how to provide any kind of security feature to these CSMA and hybrid MAC protocols. Unless security issues are resolved, TDMA MAC protocols are going to be highly vulnerable to DoS attacks if they are going to be used in the "real world" scenarios.

5.2.5 *Routing protocol attacks*

Typically, attacks against the MAC protocols might be very hard to prevent but their effects are mostly local. Attacks at the networking layer, (specifically those against the routing protocols) can disrupt the whole network operation.

The network protocols that have been proposed so far for WSSN seem to use the routing protocol of choice as geographical routing [88, 89]. Moreover, most of the few relevant papers on WMSN use geographical routing [12, 15, 90]. Nevertheless, this should not make us conclude

that this is what is going to be used in the near future. Besides the fact that these mechanisms require that nodes know their geographical positions (most of the times assuming they have a positioning system like GPS) being arguably an unfeasible requirement for many scenarios—these routing protocols have no security provisions at all. Thus, very simple attacks can be devised that will create a more global damage than the MAC attacks explored in the previous subsection.

Some routing protocols, like SAODV [55, 56], do prevent many of those attacks. SAODV uses asymmetric cryptography to authenticate each node, preventing impersonation and, in the case of a network where all the sensor nodes have the public keys of all the other nodes, detecting intrusion, efficiently.

Nevertheless, if WMSN specific routing protocols are used they have to be devised in such a way that they are resilient to security attacks. For example, distance vector routing protocols are especially vulnerable against the black hole and wormhole attacks.

Black hole attacks are one of the preferred attacks, when possible, as the attacker makes the nodes in the network think that the attacker is in the path of the most (if not all) of the routes [91]. Therefore, sending the packet to it, which the attacker can either ignore or analyze. After a while, a certain part of the network can get too congested to sustain the normal network operation.

In the wormhole attack, an attacker records messages' locations in the network and tunnels them to another attacker in a different location, which resends them into the network [92]. This creates the illusion that both attackers are one hop away from each other which increases the probabilities of the wormhole to be in a selected path when distance vector routing protocols are used.

There has been several studies trying to prevent against both the black hole attack [93–95] and the wormhole [96–98] attack. Nonetheless, more research is needed.

5.2.6 Transport layer protocols

Nowadays, different alternatives to TCP protocol adapted to the needs of the WSN are being proposed. These proposals are mainly designed to (i) make the protocols reliable and energy-efficient and (ii) provide congestion control mechanisms [99].

The transport protocol proposals for WSN include: CODA [100], GARUDA [101], PORT [102], PSFQ [103], ESRT [104], and DST [105].

Nevertheless, not all these protocols are designed to be resilient to even very simple DoS attacks that can be performed against them.

5.2.7 A concluding remark about DoS in WMSN

In conclusion, we foresee DoS attacks as one of the most important and complex challenges in security for WMSN in the near future. Even if we could be able to block all kinds of DoS but one or two, all our efforts would have been in vane.

We foresee the main trends to react to DoS attacks as the following ones: (i) not to rely on the supposed tamper-resistance of sensor nodes, (ii) use of adaptive re-routing and multi-path in the presence of jamming, collision and MAC protocol attacks, and (iii) use of routing protocols with asymmetric cryptography that is resilient to black holes, wormholes, and other similar attacks.

5.3 Traffic analysis attacks

As we have mentioned, it seems that the killer application for WMSN is going to be surveillance. A very common type of attack (just second to DoS) is going to be the traffic analysis attacks for this application.

Moreover, traffic analysis attacks are not limited to trying to eavesdrop the information the sensor network is transmitting (which can be easily prevented by the use of encryption). They can actually go much further. In this section we overview the two main traffic analysis countermeasures against the attacks that are being studied currently: concealing the geographical position of the sink and achieving event source unobservability.

5.3.1 Hiding the sink

There has been several studies trying to hide or conceal the geographical position of the sink of a WSN.

This is a specially important security feature in certain scenarios where one of the best strategies for an attacker is to geographically locate the sink and attack it physically.

In order to achieve it, different techniques to randomize communications, either during the network setup phase [106] or during the data sending phase [107], were proposed.

These schemes typically use (i) modified routing protocols that use much longer routes than needed, (ii) fake transmissions where a node acts as a sink, and (iii) creation of multiple areas of high volume communication. Obviously their main drawback is the huge overhead in transmission power and loss of bandwidth. Arguably, they are going to be used almost exclusively in military scenarios.

In addition, there has been some work directed to achieve the anonymity of both the sensor issuing an alert and the sink (or base station) [108]. Nevertheless, we don't foresee the problem of hiding geographical locations as an important problem.

5.3.2 Source location privacy

Another interesting research problem is trying to hide when (and where) an event is sensed by the network and is reported to the sink [109, 110]. This is a very complicated problem and it is highly challenging to resolve it when there exists an entity overhearing the network communications. In the case of surveillance applications a critical feature is to conceal when and where an intruder has been detected.

Alternatives that are being explored are path confusion by crossing data paths [111] and local broadcasting combined with greedy forwarding [112] among others.

More recently, the problem has been renamed as "event source unobservability" and there is some ongoing work to make it feasible even when the attacker has the required means to hear all the messages that are transmitted in the network [113].

5.4 Secure high-level data aggregation

There has been a lot of work in the area of secure data aggregation [114] and there are a variety of trade-offs need to be studied [115]. In the case of WMSN, aggregation is probably, only going to be useful with abstract information extracted from sensed media. This is because it is extremely complex to aggregate different multimedia sources into a single aggregated multimedia stream.

Still, high-level data aggregation can play a very important role in networks that have very limited network capacity (maybe because they are resisting a DoS attack). In such networks sending an aggregated data stream is preferred over sending multiple streams with highly correlated redundant information flow.

We foresee that high level data aggregation is useful especially in bandwidth critical situations.

5.5 Intruder nodes and multiple identities attacks

We foresee a future in which most of the real world scenarios will use asymmetric cryptography. In these scenarios the sink will have the identities of all (or most) of the deployed nodes with their public keys.

Before deploying a new node, the new identity and public key of the new node will be introduced to the sink, and the public key of the sink introduced to the sink.

A large amount of research papers will be published with more sophisticated and glamorous schemes that do not require sink's public key pre-loading in the sensor nodes and nodes' public key loading in the sink. Nevertheless, it is the simplest and more robust alternative.

In addition, while it can be argued that this is not the most appropriate decision for some scenarios, it does prevent intruder nodes and multiple identities attacks.

Consider, for instance, a scenario where nodes use the SAODV routing protocol [55] in conjunction with the SAKM key management scheme [56]. Moreover, new sensor nodes are deployed without proper loading of the appropriate public keys. The sink has no means to know if a particular sensor is a legitimate one or not. Many schemes can be devised to try to detect abnormal behavior, but they are going to be less reliable and introduce more hassles when compared to the case using only the aforementioned mechanisms.

Which brings us to the next research challenge: How to detect when one of those legitimate nodes is being compromised, maybe tampered and used by an intruder.

5.6 Detection of compromised nodes

Recently, many articles have been published about the problem of detection of compromised nodes. Most of them mainly focused on the problems caused by the compromised nodes trying to disrupt the normal network operation [116].

Some approaches try to identify whether or not a certain node has been compromised by a system that involves a group voting procedure [117]. Some others define so-called anomaly-based intrusion detection systems [118].

Nevertheless, most of them fail to see the fact that one of the most serious damage that a compromised node can do in a WMSN: It can just eavesdrop what the sensor network is detecting. It is just like tapping to the video surveillance security camera system of a building you are trying to rob.

In order to prevent an attacker (by compromising a very small number of intelligently selected sensor nodes) of a WMSN, from getting a fairly clear picture of what the network is sensing, schemes that ensure that each of the nodes only have very partial information would prove very valuable.

Of course, if somebody compromises a node that has a video camera there is no way to preclude the attacker to obtain the data from that camera, so expectations should be kept real.

To protect from this kind of attacks some preliminary studies have tried to solve the problem of network privacy by introducing the concept of distributed visual secret sharing [45] in which the images collected by the sensor nodes are used to generate a large number of image copies with a large amount of random noise and distributed to different nodes of the network. The image copies are generated in such a way that if an attacker captures some of them, it will not be able to create any meaningful image. On the other hand, if the sink collects most of them, it will be able to almost perfectly recreate the original image.

While this might open an interesting research field, the huge transmission overhead required by this scheme, makes very difficult to defend its feasibility in its current state.

In addition, in the case of scenarios that use clustering, the cluster heads will be an especially attractive target. Currently, there are some studies on protocols for detecting compromised cluster heads [119].

Therefore, we foresee this as a very complex and exciting research area. We believe that it will receive a considerable amount of attention in the near future.

5.7 Privacy as a security feature

Maintaining subjective privacy may be critical in surveillance applications. The idea of *subjective privacy*, introduced in [120], is that WMSN should concentrate their attention on the behavior, but not on the identity, of an individual under surveillance.

The Networked Sensor Tapestry (NeST), [120], is an architecture for secure sharing, capturing, and distributed processing of data in WMSNs. NeST is built in TinyOS and its core functionality is based on privacy filters to prevent access to personally identifiable data.

Video masking techniques may also be used, [121], to preserve privacy of authorized subjects. RFID sensors in conjunction with video sensors form a combined framework to enforce access policies to controlled spaces (i.e. buildings). In this way, a subject authorized to enter a given space is hidden in the video frames, while unauthorized subjects are not masked.

Distributed security may be obtained from coordinated cameras that obtain the same visual information [46]. The idea, based on secret sharing, consists of each camera sending partial visual information to a sink, thus providing protection against eavesdropping attacks. To obtain the whole visual information, an attacker should eavesdrop all the cameras.

In the end, since privacy requirements are going to introduce more complexity and overhead to the networking solutions, it is a trade-off. Privacy requirements might cause less secure and more resource demanding solutions. Furthermore, security solutions without considering privacy, might be too intrusive.

We believe that the right way to look at this problem is to treat privacy as just another security feature; a security feature that will be needed, or not, depending on the scenario. Although privacy has so far been grossly overlooked, in the long term it will be a part of many civil WMSNs (either due to customer and public opinion pressure or due to governmental regulations).

6 Conclusions

In this paper, we have investigated the current status of the research area of Wireless Multimedia Sensor Networks focusing on their security aspects. We have not only overviewed the current developments, but we have also given our vision of the research challenges and future trends.

We argue that DoS attacks, which are a challenging problem in WSSN security, will continue to be one of the main research challenges in WMSN. Since visual surveillance is expected to be the most important application for WMSN, traffic analysis attacks are the next challenging area for WMSN security.

Secure high-level data aggregation, intruder nodes and multiple identity attacks, detection of compromised nodes and privacy concerns constitute some of the most important security challenges that need to be addressed by WMSN in the future.

We hope that this paper will foster discussion and trigger new research ideas in an area that is just starting to show its full potential.

References

1. Akyildiz, I. F., Melodia, T., & Chowdhury, K. R. (2006). A survey on wireless multimedia sensor networks. *Computer Networks*, 921–960.
2. Girod, B., Aaron, A., Rane, S., & Rebollo-Monedero, D. (2005). Distributed video coding. In *Proc. IEEE* (Vol. 93, p. 7183). January 2005.
3. Rahimi, M., Baer, R., Iroezi, O. I., Garcia, J. C., Warrior, J., Estrin, D., & Srivastava, M. (2005). Cyclops: in situ image sensing and interpretation in wireless sensor networks. In *SenSys '05: Proceedings of the 3rd international conference on embedded networked sensor systems* (pp. 192–204). New York: ACM.
4. Kerhet, A., Magno, M., Leonardi, F., Boni, A., & Benini, L. (2007). A low-power wireless video sensor node for distributed object detection. *Journal of Real-Time Image Processing*, *2*, 331–342.
5. Kulkarni, P., Ganesan, D., Shenoy, P., & Lu, Q. (2005). SensEye: a multi-tier camera sensor network. In *MULTIMEDIA '05: Proceedings of the 13th annual ACM international conference on multimedia* (pp. 229–238). New York: ACM.
6. Zilan, R., Barcelo-Ordinas, J. M., & Tavli, B. (2008). *A survey of wireless multimedia sensor network platforms* (Technical Report: UPC-DAC-RR-XCSD-2008-12). Barcelona, Spain, September 2008.
7. Sohrabi, K., Gao, J., Ailawadhi, V., & Pottie, G. (2000). *Protocols for self-organization of a wireless sensor network*. Personal Communications, IEEE. See also *IEEE Wireless Communications*, *7*(5), 16–27.
8. Pottie, G. J., & Kaiser, W. J. (2000). Wireless integrated network sensors. *Communications of the ACM*, *43*(5), 51–58.
9. Kumar, R., Tsiatsis, V., & Srivastava, M. B. (2003). Computation hierarchy for in-network processing. In *WSNA '03: Proceedings of the 2nd ACM international conference on wireless sensor networks and applications* (pp. 68–77). New York: ACM.
10. Falemban, E., Lee, C., & Ekici, E. (2006). MMSPEED: Multipath Multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. *IEEE Transactions on Mobile Computing*, *5*(6), 738–754.
11. Mahapatra, A., Anand, K., & Agrawal, D. P. (2006). QoS and energy aware routing for real time traffic in wireless sensor networks. *Journal on Computer Communications*, *29*, 437–445.

12. Shu, L., Zhou, Z., Hauswirth, M., Phuoc, D. L., Peng, Y., & Zhang, L. (2007). Transmitting streaming data in wireless multimedia sensor networks with holes. In *MUM'07: Proceedings of the sixth international conference on mobile and ubiquitous multimedia*. New York: ACM.
13. Zhang, L., Hauswirth, M., Shu, L., Zhou, Z., Reynolds, V., & Han, G. (2008). Multi-priority multi-path selection for video streaming in wireless multimedia sensor networks. In *LNCS: Vol. 5061. UIC'08:Proceedings of the 5th international conference on ubiquitous intelligence and computing* (pp. 439–452). Berlin: Springer.
14. Sun, Y., Ma, H., Liu, L., & Zheng, Y. (2008). ASAR: an Ant-based Service Aware Routing algorithm for multimedia sensor networks. *Frontiers of Electrical and Electronic Engineering in China*, *3*(1), 25–33.
15. Campelli, L., Akyildiz, I., Fratta, L., & Cesana, M. (2008). A cross-layer solution for ultrawideband based wireless video sensor networks. In *IEEE Globecom 2008*. 30 November–4 December 2008. IEEE.
16. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM conference on computer and communications security* (pp. 41–47). New York: ACM.
17. Chan, H., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. In *IEEE symposium on security and privacy* (pp. 197–213).
18. Ramkumar, M. (2005). On broadcast encryption with random key pre-distribution schemes. In *The proceedings of the 1st int. conf. information systems security—ICISS 2005*.
19. Ramkumar, M. (2005). An efficient random key pre-distribution scheme for manet security. *IEEE Journal on Selected Areas of Communication*.
20. Liu, D., Ning, P., & Li, R. (2005). Establishing pairwise keys in distributed sensor networks. *ACM Transactions on Information and Systems Security*, *8*(1), 41–77.
21. Camtepe, S. A., & Yener, B. (2005). *Key distribution mechanisms for wireless sensor networks: a survey* (Tech. rep.).
22. Gaubatz, G., Kaps, J. P., & Sunar, B. (2004). Public key cryptography in sensor networks—revisited. In C. Castelluccia, H. Hartenstein, C. Paar, & D. Westhoff (Eds.), *Lecture notes in computer science: Vol. 3313. ESAS* (pp. 2–18). Berlin: Springer.
23. Gaubatz, G., Kaps, J. P., Ozturk, E., & Sunar, B. (2005). State of the art in ultra-low power public key. In *Proceedings of the 2nd IEEE international workshop on pervasive computing and communication security*. IEEE.
24. Watro, R., Kong, D., Cuti, S. F., Gardiner, C., Lynn, C., & Kruus, P. (2004). Tinypk: securing sensor networks with public key technology. In *SASN '04: Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks* (pp. 59–64). New York: ACM.
25. Malan, D. J., Welsh, M., & Smith, M. D. (2004). A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *Sensor and ad hoc communications and networks. IEEE SECON 2004. First annual IEEE communications society conference* (pp. 71–80).
26. Wander, A. S., Gura, N., Eberle, H., Gupta, V., & Shantz, S. C. (2005). Energy analysis of public-key cryptography for wireless sensor networks. In *Proceedings of the third IEEE international conference on pervasive computing and communications* (pp. 324–328). IEEE.
27. Piotrowski, K., Langendoerfer, P., & Peter, S. (2006). How public key cryptography influences wireless sensor node lifetime. In *Proceedings of ACM SASN*. New York: ACM.
28. Oliveira, L. B., Aranha, D., Morais, E., Daguano, F., Lpez, J., & Dahab, R. (2007). Tinytate: Computing the tate pairing in resource-constrained sensor nodes. In *Proceedings of the 6th IEEE international symposium on network computing and applications* (pp. 318–323). IEEE.
29. Oliveira, L. B., Scott, M., Lopez, J., & Dahab, R. (2008). Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. In *Proceedings of the 5th international conference on networked sensing systems*.
30. Perrig, A., Canetti, R., Song, D., & Tygar, D. (2001). Efficient and secure source authentication for multicast. In *Network and distributed system security symposium (NDSS'01)*.
31. Perrig, A., Szewczyk, R., Wen, V., Culler, D. E., & Tygar, J. D. (2001). SPINS: security protocols for sensor networks. In *Proceedings of the 7th annual international conference on mobile computing and networking* (pp. 189–199).
32. Liu, D., & Ning, P. (2004). Tesla: Broadcast authentication for distributed sensor networks. *Transactions on Embedded Computing Systems*, *3*(4), 800–836.
33. Hu, Y. C., Perrig, A., & Johnson, D. (2001). *Ariadne: A secure on-demand routing protocol for ad hoc networks* (Tech. Rep. TR01-383). Rice University.
34. Chang, S. M., Shieh, S., Lin, W. W., & Hsieh, C. M. (2006). An efficient broadcast authentication scheme in wireless sensor networks. In *Proceedings of the 2006 ACM symposium on information, computer and communications security* (pp. 311–320). New York: ACM.
35. Becher, A., Benenson, Z., & Dornseif, M. (2006). Tampering with motes: Real-world attacks on sensor networks. In *Proceedings of the 3rd international conference on security in pervasive computing*.
36. Bicakci, K., Gamage, C., Crispo, B., & Tanenbaum, A. (2005). One-time sensors: A novel concept to mitigate node-capture attacks. In *Proceedings of the 2nd European workshop on security and privacy in ad hoc and sensor networks*.
37. Misic, V. B., Fung, J., & Misic, J. (2005). Mac layer security of 802.15.4-compliant networks. In *Proceedings of the 2nd IEEE international conference on mobile ad hoc and sensor systems (IEEE MASS 2005): international workshop on wireless and sensor networks security (WSNS'05)*.
38. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's Ad-Hoc Networks Journal*, *1*(2–3), 293–315. Special Issue on Sensor Network Applications and Protocols.
39. Ganeriwal, S., Capkun, S., Han, C. C., & Srivastava, M. B. (2005). Secure time synchronization service for sensor networks. In *Proceedings of the 4th ACM workshop on wireless security* (pp. 97–106). New York: ACM.
40. Przydatek, B., Song, D., & Perrig, A. (2003). SIA: Secure information aggregation in sensor networks. In *ACM SenSys 2003*.
41. Lazos, L., & Poovendran, R. (2005). Serloc: Robust localization for wireless sensor networks. *ACM Transactions on Sensor Networks*, *1*(1).
42. Wood, A., & Stankovic, J. (2002). Denial of service in sensor network. *Computer*, *35*(10), 54–62.
43. Gruteser, M., Schelle, G., Jain, A., Han, R., & Grunwald, D. (2003). Privacy-aware location sensor networks. In *Proceedings of the USENIX 9th workshop on hot topics in operating systems* (pp. 163–167).
44. Gennaro, R., & Rohatgi, P. (2001). How to sign digital streams. *Information and Computation*, *165*, 100–116.
45. Kundur, D., Luh, W., Okorafor, U., & Zourntos, T. (2008). Security and privacy for distributed multimedia sensor networks. *Proceedings of the IEEE*, *96*(1), 112–130.
46. Luh, W., Kundur, D., & Zourntos, T. (2007). A novel distributed privacy paradigm for visual sensor networks based on sharing dynamical systems. *EURASIP Journal on Applied Signal Processing*, *2007*(1), 218.
47. Czarlinska, A., & Kundur, D. (2008). Reliable event-detection in wireless visual sensor networks through scalar collaboration and

game theoretic consideration. *IEEE Transactions on Multimedia*, *10*(5), 675–690.
48. Czarlinska, A., Luh, W., & Kundur, D. (2008). On privacy and security in distributed visual sensor networks. In *Proc. IEEE international conference on image processing (ICIP)* (pp. 1692–1695).
49. Czarlinska, A., & Kundur, D. (2008). Wireless image sensor networks: Event acquisition in attack-prone and uncertain environments. *Multidimensional Systems and Signal Processing*.
50. Lo, B. P. L., Wang, J. L., & Yang, G. Z. (2005). From imaging networks to behavior profiling: Ubiquitous sensing for managed homecare of the elderly. In *Proceedings of the pervasive computing conference* (pp. 101–104).
51. Fidaleo, D. A., Nguyen, H. A., & Trivedi, M. (2004). The networked sensor tapestry (nest): A privacy enhanced software architecture for interactive analysis of data in video-sensor networks. In *Proceedings of the ACM international workshop on video surveillance and sensor networks* (pp. 46–53).
52. Wickramasuriya, J., Datt, M., Mehrotra, S., & Venkatasubramanian, N. (2004). Privacy protecting data collection in media spaces. In *Proceedings of the ACM international conference on multimedia* (pp. 48–55).
53. Kahn, J. M., Katz, R. H., & Pister, K. S. J. (1999). Next century challenges: mobile networking for "smart dust". In *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on mobile computing and networking* (pp. 271–278). New York: ACM.
54. Lee, H. (2006). Collaborative node localization in surveillance networks using opportunistic target observations. In *ACM multimedia workshop on video surveillance and sensor networks (VSSN)*.
55. Zapata, G. M., & Asokan, N. (2002). Securing ad hoc routing protocols. In *Proceedings of the 2002 ACM workshop on wireless security (WiSe 2002)* (pp. 1–10).
56. Zapata, M. G. (2006). Key management and delayed verification for ad hoc networks. *Journal of High Speed Networks*, *15*(1), 93–109.
57. Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). *Comparing elliptic curve cryptography and rsa on 8-bit cpus* (pp. 119–132).
58. Jones, A. K., & Sielken, R. S. (1999). *Computer system intrusion detection: A survey* (Tech. rep.). University of Virginia Computer Science Department.
59. Huang, Y., & Lee, W. (2003). A cooperative intrusion detection system for ad hoc networks. In *SASN '03: Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks* (pp. 135–147). New York: ACM.
60. Barford, P., Jha, S., & Yegneswaran, V. (2004). Fusion and filtering in distributed intrusion detection systems. In *Proceedings of the 42nd annual Allerton conference on communication, control and computing*.
61. Marks, D. G., Mell, P., & Stinson, M. (2004). Optimizing the scalability of network intrusion detection systems using mobile agents. *Journal of Network and Systems Management*, *12*(1), 95–110.
62. Anderson, R., & Kuhn, M. (1996). Tamper resistance—a cautionary note. In *Proceedings of the second Usenix workshop on electronic commerce*.
63. Anderson, R., & Kuhn, M. (1997). Low cost attacks on tamper resistant devices. In *LNCS. IWSP: International workshop on security protocols*. Berlin: Springer.
64. Biham, E., & Shamir, A. (1997). Differential fault analysis of secret key cryptosystems. In *CRYPTO* (pp. 513–525).
65. Mohammed, L. A., & Issac, B. (2007). Detailed DoS attacks in wireless networks and countermeasures. *International Journal of Ad Hoc and Ubiquitous Computing*, *2*(3), 157–166.
66. Law, Y. W., van Hoesel, L., Doumen, J., Hartel, P., & Havinga, P. (2005). Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. In *SASN '05: Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks* (pp. 76–88). New York: ACM.
67. Xu, W., Trappe, W., & Zhang, Y. (2007). Channel surfing: defending wireless sensor networks from interference. In *IPSN '07: Proceedings of the 6th international conference on information processing in sensor networks* (pp. 499–508). New York: ACM.
68. Xu, W., Trappe, W., & Zhang, Y. (2008). Defending wireless sensor networks from radio interference through channel adaptation. *ACM Transactions on Sensor Networks*, *4*(4), 1–34.
69. Xu, W., Ma, K., Trappe, W., & Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies. *Network, IEEE*, *20*(3), 41–47.
70. Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In *MobiHoc '05: Proceedings of the 6th ACM international symposium on mobile ad hoc networking and computing* (pp. 46–57). New York: ACM.
71. Xu, W., Wood, T., Trappe, W., & Zhang, Y. (2004). Channel surfing and spatial retreats: defenses against wireless denial of service. In *WiSe '04: Proceedings of the 3rd ACM workshop on wireless security* (pp. 80–89). New York: ACM.
72. Thamilarasu, G., Balasubramanian, A., Mishra, S., & Sridhar, R. (2005). A cross-layer based intrusion detection approach for wireless ad hoc networks. In *IEEE international conference. Mobile adhoc and sensor systems conference* (p. 7).
73. Zhou, Y., Wu, D., & Nettles, S. M. (2006). On MAC-layer denial of service attacks in IEEE 802.11 ad hoc networks: analysis and counter measures. *International Journal of Wireless and Mobile Computing*, *1*(3/4), 268–275.
74. Guang, L., & Assi, C. (2005). On the resiliency of mobile ad hoc networks to MAC layer misbehavior. In *PE-WASUN '05: Proceedings of the 2nd ACM international workshop on performance evaluation of wireless ad hoc, sensor, and ubiquitous networks* (pp. 160–167). New York: ACM.
75. Guang, L., Assi, C., & Ye, Y. (2007). DREAM: A system for detection and reaction against MAC layer misbehavior in ad hoc networks. *Computer Communications*, *30*(8), 1841–1853.
76. Radosavac, S., Cárdenas, A. A., Baras, J. S., & Moustakides, G. V. (2007). Detecting IEEE 802.11 MAC layer misbehavior in ad hoc networks: Robust strategies against individual and colluding attackers. *Journal of Computer Security*, *15*(1), 103–128.
77. Aad, I., Hubaux, J. P., & Knightly, E. W. (2004). Denial of service resilience in ad hoc networks. In *MobiCom '04: Proceedings of the 10th annual international conference on mobile computing and networking* (pp. 202–215). New York: ACM.
78. Bicakci, K., & Tavli, B. (2009). Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards and Interfaces*.
79. Demirkol, I., Ersoy, C., & Alagoz, F. (2006). MAC protocols for wireless sensor networks: a survey. *IEEE Communications Magazine*, *44*(4), 115–121.
80. Bai, R. G., Qu, Y. G., Guo, Y., Zhao, B. H. (2007). An energy-efficient TDMA MAC for wireless sensor networks. In *The 2nd IEEE Asia-Pacific service computing conference* (pp. 69–74).
81. De Rango, F., Perrotta, A., & Marano, S. (2007). QoS-CROMA: An on-demand time-slotted MAC protocol with QoS support for wireless ad hoc networks. In *4th international symposium on wireless communication systems. ISWCS 2007* (pp. 706–710).
82. Li, W., Wang, S., & Wei, J. B. (2008). An evolutionary topology unaware TDMA MAC protocol for ad hoc networks. In *IEEE international conference on communications. ICC '08* (pp. 4825–4829).

83. Lessmann, J. (2007). GMAC: A position-based energy-efficient QoS TDMA MAC for ad hoc networks. In *15th IEEE international conference on networks. ICON 2007* (pp. 449–454).
84. Rhee, I., Warrier, A., Aia, M., & Min, J. (2005). Z-MAC: a hybrid MAC for wireless sensor networks. In *SenSys '05: Proceedings of the 3rd international conference on embedded networked sensor systems* (pp. 90–101). New York: ACM.
85. Wang, W., Wang, H., Peng, D., & Sharif, H. (2006). An energy efficient pre-schedule scheme for hybrid CSMA/TDMA MAC in wireless sensor networks. In *10th IEEE Singapore international conference on communication systems. ICCS 2006* (pp. 1–5).
86. Tavli, B., & Heinzelman, W. (2004). Mh-trace: Multi-hop time reservation using adaptive control for energy efficiency. *IEEE Journal on Selected Areas in Communications*, *22*, 942–953.
87. Tavli, B., & Heinzelman, W. (2006). *Mobile ad hoc networks: energy-efficient real-time group communications*. Berlin: Springer. ISBN 1-4020-4632-4.
88. Seada, K., Zuniga, M., Helmy, A., & Krishnamachari, B. (2004). Energy-efficient forwarding strategies for geographic routing in lossy wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on embedded networked sensor systems* (pp. 108–121). New York: ACM.
89. Zhang, R., Zhao, H., & Labrador, M. A. (2006). The Anchor Location Service (ALS) protocol for large-scale wireless sensor networks. In *InterSense '06: Proceedings of the first international conference on integrated Internet ad hoc and sensor networks* (p. 18). New York: ACM.
90. Ma, C., & Yang, Y. (2006). Battery aware routing for streaming data transmissions in wireless sensor networks. *Mobile Networks and Applications*, *11*, 757–767.
91. Al-Shurman, M., Yoo, S. M., & Park, S. (2004). Black hole attack in mobile ad hoc networks. In *ACM-SE 42: Proceedings of the 42nd annual southeast regional conference* (pp. 96–97). New York: ACM.
92. Hu, Y. C., Perrig, A., & Johnson, D. (2006). Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, *24*(2), 370–380.
93. Weerasinghe, H., & Fu, H. (2007). Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. *Future Generation Communication and Networking*, *2*, 362–367.
94. Djahel, S., Nait-Abdesselam, F., & Khokhar, A. (2008). An acknowledgment-based scheme to defend against cooperative black hole attacks in optimized link state routing protocol. In *IEEE international conference on communications ICC '08* (pp. 2780–2785).
95. Djenouri, D., & Badache, N. (2008). Struggling against selfishness and black hole attacks in MANETs. *Wireless Communications and Mobile Computing*, *8*(6), 689–704.
96. Poovendran, R., & Lazos, L. (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wireless Networks*, *13*(1), 27–59.
97. Moss, C., & Evans, D. W. (2005). Securing wireless communication against wormhole attacks. In *EHAC'05: Proceedings of the 4th WSEAS international conference on electronics, hardware, wireless and optical communications* (pp. 1–6). Stevens Point: World Scientific and Engineering Academy and Society (WSEAS).
98. Choi, S., Kim, D. Y., Lee, D. H., & Jung, J. I. (2008). WAP: Wormhole attack prevention algorithm in mobile ad hoc networks. In *IEEE international conference on sensor networks, ubiquitous and trustworthy computing. SUTC '08* (pp. 343–348).
99. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Computer Networks*, *52*(12), 2292–2330.
100. Wan, C. Y., Eisenman, S. B., & Campbell, A. T. (2003). CODA: congestion detection and avoidance in sensor networks. In *SenSys '03: Proceedings of the 1st international conference on embedded networked sensor systems* (pp. 266–279). New York: ACM.
101. Park, S. J., Vedantham, R., Sivakumar, R., & Akyildiz, I. F. (2004). A scalable approach for reliable downstream data delivery in wireless sensor networks. In *MobiHoc '04: Proceedings of the 5th ACM international symposium on mobile ad hoc networking and computing* (pp. 78–89). New York: ACM.
102. Zhou, Y., Lyu, M., Liu, J., & Wang, H. (2005). PORT: A price-oriented reliable transport protocol for wireless sensor networks. In *16th IEEE international symposium on software reliability engineering, ISSRE 2005* (p. 10).
103. Wan, C. Y., Campbell, A., & Krishnamurthy, L. (2005). Pump-slowly, fetch-quickly (PSFQ): a reliable transport protocol for sensor networks. *IEEE Journal on Selected Areas in Communications*, *23*(4), 862–872.
104. Özgür, B. Akan, & Akyildiz, I. F. (2005). Event-to-sink reliable transport in wireless sensor networks. *IEEE/ACM Transactions on Networks*, *13*(5), 1003–1016.
105. Gungor, V., & Akan, O. (2006). DST: delay sensitive transport in wireless sensor networks. In *International symposium on computer networks* (pp. 116–122).
106. Wadaa, A., Olariu, S., Wilson, L., Eltoweissy, M., & Jones, K. (2004). On providing anonymity in wireless sensor networks. In *ICPADS '04: Proceedings of the parallel and distributed systems, tenth international conference* (p. 411). Washington: IEEE Computer Society.
107. Deng, J., Han, R., & Mishra, S. (2005). Countermeasures against traffic analysis attacks in wireless sensor networks. In *SECURECOMM '05: Proceedings of the first international conference on security and privacy for emerging areas in communications networks* (pp. 113–126). Washington: IEEE Computer Society.
108. Ouyang, Y., Le, Z., Xu, Y., Triandopoulos, N., Zhang, S., Ford, J., & Makedon, F. (2007). Providing anonymity in wireless sensor networks. In *IEEE international conference on pervasive services* (pp. 145–148).
109. Ozturk, C., Zhang, Y., & Trappe, W. (2004). Source-location privacy in energy-constrained sensor network routing. In *SASN '04: Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks* (pp. 88–93). New York: ACM.
110. Kamat, P., Zhang, Y., Trappe, W., & Ozturk, C. (2005). Enhancing source-location privacy in sensor network routing. In *ICDCS '05: Proceedings of the 25th IEEE international conference on distributed computing systems* (pp. 599–608). Washington: IEEE Computer Society.
111. Hoh, B., & Gruteser, M. (2005). Protecting location privacy through path confusion. In *First international conference on security and privacy for emerging areas in communications networks, SecureComm 2005* (pp. 194–205).
112. Xi, Y., Schwiebert, L., & Shi, W. (2006). Preserving source location privacy in monitoring-based wireless sensor networks. In *20th international parallel and distributed processing symposium, IPDPS 2006* (p. 8).
113. Yang, Y., Shao, M., Zhu, S., Urgaonkar, B., & Cao, G. (2008). Towards event source unobservability with minimum network traffic in sensor networks. In *WiSec '08: Proceedings of the first ACM conference on wireless network security* (pp. 77–88). New York: ACM.
114. Alzaid, H., Foo, E., & Nieto, J. G. (2008). Secure data aggregation in wireless sensor network: a survey. In *AISC '08: Proceedings of the sixth Australasian conference on information security* (pp. 93–105). Darlinghurst: Australian Computer Society.
115. Solis, I., & Obraczka, K. (2006). In-network aggregation trade-offs for data collection in wireless sensor networks. *International Journal of Sensor Networks*, *1*(3/4), 200–212.

116. Zhang, Q., Yu, T., & Ning, P. (2008). A framework for identifying compromised nodes in wireless sensor networks. *ACM Transactions on Information and Systems Security*, *11*(3), 1–37.
117. Li, T., Song, M., & Alam, M. (2008). Compromised sensor nodes detection: A quantitative approach. In *ICDCSW '08: Proceedings of the 2008 the 28th international conference on distributed computing systems workshops* (pp. 352–357). Washington: IEEE Computer Society.
118. Mathews, M., Song, M., Shetty, S., & McKenzie, R. (2007). Detecting compromised nodes in wireless sensor networks. In *ACIS international conference on software engineering, artificial intelligence, networking, and parallel/distributed computing* (Vol. 1, pp. 273–278).
119. Krauß, C., Stumpf, F., & Eckert, C. (2007). *Detecting node compromise in hybrid wireless sensor networks using attestation techniques* (pp. 203–217).
120. Fidaleo, D. A., Nguyen, H., & Trivedi, M. (2004). The networked sensor tapestry (nest): A privacy enhanced software architecture for interactive analysis of data in video-sensor networks. In *ACM 2nd international workshop on video surveillance & sensor networks (VSSN)*.
121. Wickramasuriya, J., Datt, M., Mehrotra, S., & Venkatasubramanian, N. (2004). Privacy protecting data collection in media spaces. In *Proceedings of the 12th annual ACM international conference on multimedia*. New York: ACM.

Manel Guerrero-Zapata is an Assistant Professor in the Computer Architecture Department (DAC) at the Technical University of Catalonia (UPC).
His research interests include network security, wireless networks, and routing protocols. He is the author of Secure Ad hoc On-Demand Distance Vector (SAODV) routing protocol and of Simple Ad hoc Key Management (SAKM) scheme.
He received his Ph.D., M.S. and B.S. in Computer Science from the Technical University of Catalonia (UPC) in 2006, 1999 and 1997 respectively.
From 1998 to 2003 he worked at the Nokia Research Center in Helsinki (first as Assistant Research Engineer, then as Research Scientist, and finally as Senior Research Scientist). From 2003 to 2005 he worked as an assistant professor at the Universitat Pompeu Fabra (UPF) in Barcelona.

Ruken Zilan received the B.S. and M.S. degrees in Physics respectively, in 1997 from Gazi University and in 2001 from Middle East Technical University, Ankara Turkey. She received her 2nd M.S. degree in Computer Engineering from TOBB University of Economics and Technology, Ankara Turkey, in 2007.
She is currently pursuing her Ph.D. in Computer Architecture Department, Technical University of Catalonia (UPC), Barcelona, Spain, as a member of CompNET Research Group at UPC. She is also a member of Barcelona Super Computing Center, as a CISCO scholar.
Her research interests are network processors, Internet traffic, wireless networks, wireless multimedia sensor networks, computer vision, image processing.

José M. Barceló-Ordinas is an Associate Professor in the Computer Architecture Department (DAC) at UPC. He received his Ph.D. and Ms.C. in Telecommunications Engineering at Universidad Politecnica de Catalunya (UPC) in 1998 and 1991 respectively.
He joined the CompNet group at the Computer Architecture Department in 1993. He has participated in several European projects such as EXPLOIT, BAF, EXPERT, NETPERF, MOEBIUS, WIDENS projects, and EuroNGI, EuroNFI and EuroNF (VII FP) Networks of Excellence (NoE).
His currently research areas are DTN (Delay Tolerant Networks), VANETs (Vehicular Ad Hoc Networks) and WMSN (Wireless Multimedia Sensor Networks).

Kemal Bicakci is an Assistant Professor at the Department of Electrical and Electronics Engineering, TOBB (The Union of Chambers and Commodity Exchanges of Turkey) University of Economics and Technology. He has obtained his Ph.D. degree from Middle East Technical University, Ankara, Turkey in 2003. Between 2004 and 2006, he was a postdoc researcher in Vrije Universiteit Amsterdam working with Prof. Tanenbaum in EU FP6 project named SecurE-Justice. His previous research experience includes several NSF funded security projects in which he participated as a research assistant during his MS studies in University of Southern California, Los Angeles, USA. His research interests include information security, applied cryptography, wireless and sensor networks and medical informatics.

Bulent Tavli is an Assistant Professor in the Department of Computer Engineering at the TOBB University of Economics and Technology, Ankara, Turkey. He received the B.S. degree in Electrical and Electronics Engineering in 1996 from the Middle East Technical University, Ankara, Turkey. He received the M.S. and Ph.D. degrees in Electrical and Computer Engineering in 2001 and 2005 from the University of Rochester, Rochester, NY, USA. Telecommunications, networking, signal processing, and embedded systems are his current research areas.