Secure Wireless Multimedia Sensor Networks: a Survey

Luigi Alfredo Grieco and Gennaro Boggia
Dipartimento di Elettrotecnica ed Elettronica
Politecnico di Bari
Bari, Italy
a.grieco@poliba.it
g.boggia@poliba.it

Sabrina Sicari and Pietro Colombo
Dipartimento di Informatica e Comunicazione
Università degli studi dell'Insubria
Varese, Italy
sabrina.sicari@uninsubria.it
pietro.colombo@uninsubria.it,

Abstract—**The application domains of Wireless Multimedia Sensor Networks (WMSNs) range over multimedia surveillance systems, traffic monitoring and control in urban/suburban areas, support to military and/or anti-terrorism operations, telemedicine, assistance to disabled and/or elderly people, environmental monitoring, secure localization of services and users, industrial process control. In order to ensure a broad deployment of such innovative services, strict requirements on security, privacy, and distributed processing of multimedia contents should be satisfied, taking also into account the limited technological resources (in term of energy, computation, bandwidth, and storage) of sensor nodes. Thus, with respect to classic Wireless Sensor Networks, the achievement of these goals is more challenging due to the presence of multimedia data, which usually requires complex compression and aggregation algorithms. In order to provide a unifying synthesis on the last achievements, this survey summarizes the main findings on secure WMSNs proposed in the literature and forecasts future perspectives of such a technology.**

Keywords - Security, Wireless Multimedia Sensor Network, Privacy, Secure Aggregation.

I. INTRODUCTION

The high and ever growing availability of low cost multimedia devices (such as videocamera and microphones with CMOS technology) and wireless communication systems (such as those proposed by the families of standards IEEE 802.11 and 802.15 [4]) fostered the development of Wireless Multimedia Sensor Networks (WMSNs). The CMOS technology allows one to embed into a unique device a lens, an optic sensor and the logic components that are required for the execution of algorithms to process digital signals, such as the ones that are used for images' stabilization and compression [8]. Such an input device can be connected (for instance, by means of modules Cyclops [9]) to already available wireless sensors (for instance Crossbow, MICA2 or MICAZ [10]). The resulting connection is a multimedia sensor equipped with images acquisition and processing functionalities, communication interfaces, memory modules, power supply and control units [3]. Imote, Imote2 and Stargate are some other examples of recently released multimedia sensors [10,19]. A WMSN is composed of numerous multimedia sensors that exchange sensed data with sinks using a wireless channel (see Fig. 1). WMSNs are used in many contexts and therefore their application domains are continuously growing: they range over indoor/outdoor surveillance systems, traffic monitoring and control systems for urban and sub-urban areas, systems supporting telemedicine, attendance to disable and elderly people, environment monitoring, localization and recognition of services and users, monitoring and control of manufacturing processes in industry [1, 69]. Such services could also integrate geographical wireless communication technologies such as 3G or LTE [5, 6]. Moreover, the presence of multiple video sensors allows one to extend the artificial field of vision by means of numerous points of view, and also to use sensors with different resolution for an analysis of the monitored fields based on different qualitative levels [1, 3].

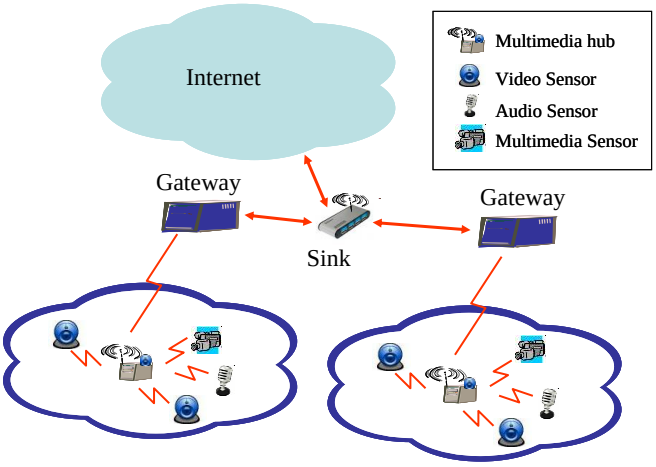

Figure 1: Wireless Multimedia Sensor Networks Architecture.

The requirements of the multimedia monitoring applications state new problems that the wireless communication and processing infrastructures have to solve to assure the desired Quality of Experience (QoE). Such problems include the limited power resources and computational capabilities [8-10,14], the computational complexity of compression,

aggregation, and distributed processing, the overload to manage security/privacy policies and Quality of Service (QoS).

With respect to classic Wireless Sensor Networks (WSNs), the constraints, imposed by the computational capacity, the memory and energy resources, become more critical. In fact, in the context of WMSNs, security and privacy policies have to be combined with complex algorithms for compression and distributed processing of multimedia contents. As a consequence, WMSNs require tools and methodologies different from the ones proposed for common WSNs [2]. The innovative features of this research field are also underlined by the promising technological innovations in the area of nano-technologies, that can significantly increase the computational capabilities of sensors [42,59].

Although the international scientific community has proposed interesting architectural and technological solutions [15-18], a lot of work is required to build secure WMSNs. In fact, in order to ensure a wide deployment of WMSN-based services in the real world, the whole WMSN paradigm should be reformulated by having security and privacy as fundamental requirements. In other words, each single algorithm and/or technology employed in this kind of networks have to be designed by properly taking into account security and privacy. From now on, we will refer to this design rule as *integrated approach* that is a design considering a security framework in which all WMSN requirements are satisfied.

Many works in the literature concern the processing of images (compression, extraction, analysis and aggregation) [23-26], some works concern the problem to transmit multimedia contents by means of wireless networks [27, 28], and therefore while other works are focused on real-time applications [11, 12]. Notice that although privacy and security policies play a fundamental role in the context of WMSN applications, they are often underestimated whenever new algorithms or architectural and technological solutions are proposed [1, 7]. For instance, consider the high critical, sensitive and reserved information managed by networks that support telemedicine or monitoring services in countries threatened by terrorism. The research on secure WMSNs is oriented to the definition of solutions that, depending on the application context, adequately satisfy the requirements of security, privacy, and quality of the transmitted data as well as power consumption.

To provide a comprehensive view of the contributions of the scientific community in this field and to accelerate their future convergence towards unifying solutions, this survey summarizes the main findings on secure WMSNs and forecasts future perspectives of such a technology. In particular, our work is mainly conceived to discuss in depth about existing and/or upcoming solutions for open security issues in WMSNs. With respect to previous surveys on WSNs and WMSNs, such as [1, 7, 41, 60, 69, 72, 74], which are mainly devoted to the analysis of general security issues and DoS attacks, the attention here will be focused on scientific proposals for authentication, secure node localization, privacy policies, trust management, and data aggregation/compression, which have been explicitly conceived to face with security and privacy, or which can be easily extended to cope with them. We highlight that we will separately show the study of these issues, but an effective WMSN design requires the integrated approach mentioned above. More specifically, the future direction of research for secure wireless multimedia sensor network should satisfy not only a specific security requirement, but all the security/privacy and quality of service issues.

The work is organized as follows: Section II focuses on authentication mechanisms, secure localization algorithms and trust management; Section III deals with privacy aspects; Section IV faces with secure compression and aggregation algorithms. Finally, Section V discusses future research directions and states final considerations.

II. Authentication, Secure Localization and Trust Management

So far only a part of the security solutions used in WMSNs fully complies with the peculiarities of these networks. In fact, in some cases, known schemes of WSN can be effectively reused without any significant modifications. In other cases, instead, the schemes adopted in WSN could be improved by leveraging on the capabilities of multimedia sensors. In particular, this is true when we consider authentication, node localization, and, in general, trust management. Solutions to these problems are typically inherited from WSNs. But we need to characterize them with respect to the new application context.

It is well known that wireless communications make security and privacy requirements critical because they increase the vulnerabilities and the threats on the integrity and confidentiality of the transmitted data. For these reasons, authentication mechanisms [20] are required to guarantee the correctness and the confidentiality of data. For instance, watermarking technique is an effective vehicle to assert and assure the image data authentications [20]. Moreover, due to the high number of sensor nodes, such systems could contain control units that broadcast commands and data to the nodes. As a consequence, the authenticity of these data and commands is a critical requirement for the correct behaviour of a WMSN. Actually, it is really a complex problem to guarantee the correct broadcast authentication of the messages transmitted by control units, since the broadcast authentication algorithms that are currently available in the literature [31-33] do not adequately satisfy the QoS requirements of multimedia signals.

At present, no solution is specifically deployed for WMSNs. Therefore, new approaches exploiting the characteristics of multimedia nodes should be developed. In particular, it is now possible to think at new solutions based on public key digital signature schemes [75]. The capabilities of multimedia nodes can be used to simplify the authentication procedures and to realize more effective key management

approaches based on asymmetric cryptography. This research direction could be supported by nanotechnology based solutions, which promise to greatly enhance the capabilities of sensor nodes [42]. In the literature some schemes [76, 77] have been proposed in the field of wireless sensor networks, but they cannot be effectively applied to WSN due to the memory and processing limitations of sensors. On the contrary WMSN sensors should be able to support new solutions based on multimedia content (e.g., schemes based on watermaking [20,21]) .

According to the proposed vision of an integrated design approach, the problem of the authentication is strictly related to the secure node localization issue, given that authentication can be used to ensure reliable information. Due to the distributed nature of WMSNs, in several application scenarios [34, 35] the localization of the multimedia sensors is required to assure the supply of the services. Therefore, the integrity and confidentiality of localization information are fundamental and it is necessary to define countermeasures versus possible malicious attacks. Authentication mechanisms can improve the security of the localization information, but they are not enough to guarantee the complete reliability of the contained information [36]. Moreover, although further approaches were defined to address such an issue [37, 38], they do not adequately satisfy some requirements, such as the real time scheduling constraints imposed by some multimedia applications.

Issues of authentication and secure localization information fall in the general problem of the trust management. In a distributed and collaborative environment like a WMSN, trust management becomes a real challenging aspect. The analysis of the trust relationships among the components of a network drives one to choose ad hoc security oriented countermeasures that aim at guaranteeing the protection of data, the secure routing, the exchange of localization information, and so on. However, the definition of an effective model of trust becomes a complex task in a highly distributed environment characterized by strict performance requirements. Each node should be equipped with an autonomous evaluation and analysis capabilities that aim at measuring the trust relationships with the other members of the network; notice that such relationships depend on the communication and cooperation needs of the nodes. In other words, it is required to move from the classic centralized and static approach proposed for the most widely used trust management solutions, to adopt a fully distributed and dynamic approach that assumes that no trust relationship is defined a priori among the nodes of the network. At present only few solutions are available [39-40], but they cannot be applied to WMSNs due to the relevant computational effort required by the multimedia traffic and to the real-time constraints that are not suited to the limited power resources of current sensor nodes.

III. PRIVACY

WMSNs handle and collect a great amount of data of different nature, which may provide some kind of information on individuals in both a direct or indirect form, i.e., they may specify explicit information on individuals, or they may be used to infer information on them. As a consequence, under some circumstances, data may be used to violate the privacy of individuals.

Privacy has received increasing attention from companies, researchers and legislators. Legislative acts, such as the European Union Directive for personal data [51], the Health Insurance Portability and Accountability Act for healthcare data [52] and the Gramm Leach Bliley Act [53] for financial institutions, require governments and enterprises to protect the privacy of their citizens and customers, respectively.

Privacy is a key requirement for numerous application scenarios of WMSN. As an example consider the systems of telemedicine or of military surveillance. In both the cases, data are sensitive and are required to be adequately protected. In other words, in such contexts it is fundamental to guarantee the confidentiality of the communication among the nodes within the network and between the nodes and the sink.

WMSNs run the risk of individual privacy violation due to possible unauthorized access to data that are handled by the networks. This threat is mainly attributable to vulnerabilities of WMSN such as the wireless nature of the communication channels, the remote access to data and the huge quantity of multimedia data that are exchanged within the network. Notice that with respect to traditional WSN the data traffic is far bigger, hence it may be more easily to perform privacy attacks.

Attacks versus privacy that exploit these vulnerabilities can be classified into two distinct macro-types of techniques [43,44]:

- *Eavesdropping*. Due to the wireless communication channel, data can be discovered (and used to attack the privacy of individuals referred to by those) by sniffing the messages exchanged by the network nodes.
- *Masquerading*. Data can be retrieved by means of some malicious nodes that misroute the packets and mask their real nature behind the identity of nodes that are authorized to take part to communication.

The design of privacy protecting mechanisms is a challenging problem for the intrinsic characteristics of wireless multimedia sensor networks. More specifically, it is required to take into account the limited computational capabilities of the sensor nodes as well as the low power resources of sensors. Moreover, it is necessary that privacy enabling solutions do not affect the quality of service, as an example in case of video streaming applications it is fundamental that the privacy solutions do not compromise the fluency of the transmission.

The literature reports three different types of solutions that aim at hindering such attacks: anonymity mechanisms based on data cloaking [43, 47], privacy aware mechanisms based

on secure communication channels [45] and privacy policy based approaches [50]. Some of the proposed solutions are specifically designed for WMSNs, other are designed for a generic WSN or are general privacy solutions that can be also applied to WMSNs.

A. Data cloaking

Data cloaking anonymity mechanisms aim at hiding the informative content of messages by perturbing data according to specific patterns/criteria.

Some data cloaking approaches, which were specifically designed for WSN, but can be also applied to WMSN, are the ones proposed in [43, 46-48]. These works concern mechanisms to decentralize sensitive data. More specifically, the basic idea of the former approach is to distribute the sensed location data through a spanning tree. Each node handles only a part of the original sensed data and no node holds the complete view of the original data. In this case the cloaking is made by splitting the data in multiple chunks. Notice that such a technique is very effective against eavesdropping. In order to retrieve the complete data that might allow one to execute privacy attacks, one should sniff the communication of all the nodes of the spanning tree.

Other cloaking techniques proposed in the literature are expressly dedicated to protect the localization of nodes [43, 46, 85, 86]. Notice that although these solutions are not specifically defined for WMSN, they can be applied to these networks whenever it is required to deal with localization data provided in conjunction with multimedia content, for instance in case a multimedia node is also equipped with a GPS component. For instance, [43] proposes a solution that guarantees the anonymous usage of location based information. The solution consists of an algorithm, which regulates the granularity of location information to meet certain specified anonymity constrains. In this case the cloaking is operated by obfuscating some details of the sensed data. Another work [87] proposes an approach that alters the traffic pattern with some bogus data that obfuscate the real position of the nodes. In this case the cloaking consists in the additional artificial noise.

A similar technique, proposed in [81], is expressly designed to enable privacy in vision rich systems built on WMSNs. Another example of data cloaking is provided by Lo et al. [79] that introduce an automated homecare monitoring system for the elderly, named UbiSense. The UbiSense WMSN employs low-cost video sensors embedded in the environment along with body sensors and radiofrequency identification (RFID) in order to conduct gait and posture recognition of the elderly. Monitoring of changes in gait and posture provides telltale signs of the onset of a physical accident or disease, providing an automated way to alert necessary caregivers when needed. To address the invasive nature of this approach, image processing is conducted directly at the camera that converts the video information into abstractions containing only shape and outline information necessary to recognize gait and posture anomalies. Only the abstractions are communicated and processed within the network, assuring a form of privacy.

The work of [81] describes another interesting distributed cloaking approach for WMSN. The proposed approach combines solutions of signal processing, networking and cryptography. Each visual sensor in a cluster acquires correlated data and generates a share that is transmitted to the BS (Base Station) along disjoint multi-hop paths. The BS reconstructs aggregated data, given most of the shares, while a corrupt node cannot, given its limited access to a small fraction of shares. In the network no sensors have a complete vision, a complete knowledge, but only partial information. In this way the network is protected from both privacy attacks. The algorithm proposed in [81] sacrifices unconditional secrecy to provide a lightweight security solution realizable for lower cost sensors. The solutions is based on a visual secrecy measure that degrades proportionally to the number of shares of an eavesdropper. Such a relaxed definition of secrecy is based on an distortion perceived by an eavesdropper and has been proposed in the literature [83]. The definition reduces the complexity of pixel-by-pixel computations and reduces the size of the shares in comparison to traditional visual secret-sharing solutions [84] reducing storage and bandwidth complexity, which are of great importance in WMSNs.

B. Secure communication channels

A further approach is based on the usage of secure communication protocols to hinder eavesdropping and active attacks. In this case the cloaking is executed by means of encryption techniques. The aim of this technique is to guarantee the confidentiality of data by hiding their actual content.

Some solutions such as the protocol SPINS [45] originally designed for generic WSN can also be applied to WMSN; other proposals, like [80], are specifically defined for WMSN. Fidaleo et al. [80] introduce the networked sensor tapestry (NeST) architecture designed for the secure sharing, capture, distributed processing, and archiving of multimedia data. The NeST infrastructure is developed to facilitate the fast prototyping and deployment of WMSNs for a wide variety of surveillance applications including battlefield assistance and structural monitoring. To facilitate societal trust in WMSNs, the authors introduce the notion of Bsubjective privacy in video where the behavior, but not the identity, of an individual under surveillance is conveyed. Their approach to privacy involves processing of the raw sensor data in order to remove personally identifiable information. The resulting data, approved for public viewing, are communicated in a network that employs the secure socket layer protocol (SSL) [88] and client authorization for network level protection.

C. *Privacy policy based approaches*

An alternative solution to cloaking and secure communication channels is represented by policy based techniques.

In order to use WMSNs as indispensable tools of every day life it is required that their nodes comply with privacy policies, which aim at protecting the handled and transmitted data. Privacy policy based approaches [50, 54-56] state who can use individuals data, which data can be collected, for what purpose the data can be used, and how they can be distributed.

A common policy based approach addresses privacy concerns after data have been collected [56]. In other words, this type of solution is provided for sinks that receive data from nodes and have to handle such data adequately. Notice that this solution do not assure the privacy during the communication phase, as a secure communication channel solution makes, hence it may be subject of both eavesdropping and active attacks. However, it can be used in combination with other policy based or data cloaking solutions.

Wickramasuriya et al. [82] present a privacy-preserving video surveillance system that monitors subjects in an observation region using video cameras along with localized sensors. The localized sensors include RFID tags that wearied by subjects and motion detectors placed within the observation environment. The motion detectors are used to turn the video cameras on or off, while the RFIDs of the subjects provide information that specify which individuals are entitled to privacy. The information from the various sensors is fused with the video data, resulting in a video stream with only authorized subjects being masked through image processing.

Other works [49] address the access control and authentication issues, for instance Duri et al. [50] propose a policy-based framework for protecting sensor information. At present the existent solutions that guarantee the privacy of data in the context of WMSNs are still in a primitive state and many open problems still exist and are yet to be discovered, hence, further research work is required in this field [29, 30, 81].

IV. Secure Compression and Aggregation of Multimedia Contents

Compression techniques and aggregation algorithms for multimedia contents are crucial to reduce the amount of transmitted data and to save energy and processing resources in WMSNs. So far, many compression schemes have been proposed as described in the surveys [60, 72]. Nevertheless, the problem of aggregating multiple compressed frames coming from different video sensors while guaranteeing the expected security level is still a open research area. In fact, due to the complex compression operations, the distributed elaboration of the multimedia contents and the limited bandwidth and power resources of WMSNs, it is necessary to introduce secure aggregation algorithms that decrease the total amount of information to elaborate, transmit, and protect at the same time the quality of the multimedia message. The literature provides a great variety of end-to-end and hop-by-hop secure aggregation protocols [89]; Wang et al. [41] propose a survey on the most important solutions, but they can be hardly applied to multimedia data. For instance, the encryption of images is a highly power consuming task [21], hence the most innovative solutions come to the arrangement to adopt selective encryption schemes for the multimedia contents [22, 62-66]. In such contexts, thanks to the flexibility of standard codings such as JPEG2000 [13], it is possible to describe an image as composed of different and mutual integrable qualitative levels, and to encrypt only the data of the basic level, by making useless any attack oriented to the theft of no encrypted transmitted data [61]. A possible research direction is based on exploiting compression algorithms that do not strictly require entropy coding, such as Set-Partitioning In Hierarchical Trees image. In fact, since entropy coding requires a high computational effort, the energy efficiency of the WMSN would be improved [72, 73].

To take into account the costs deriving from the secure aggregation of multimedia contents, in [67] a method for optimizing the placement of aggregation nodes has been proposed. It consists in a distributed algorithm that dynamically setups and modifies aggregation routes by taking into account both transmission and aggregation costs. The algorithm is a distributed version of the offline Adaptive Fusion Steiner Tree algorithm [68], whose rationale is to perform data aggregation when there exists sufficient data redundancy to justify the costs deriving from the aggregation.

In [70] a method has been conceived to discard video frames by taking into account both the node status and the impact of frame losses on the overall video distortion. It is based on an advanced prediction model of H.264 video sequences [71]. By applying it, each node of a WMSN is able to select which video frame can be discarded without a significant impact on the overall video quality, thus allowing the finding of an optimal trade-off among resource consumption and QoE.

Starting from this big picture, it appears that research on secure aggregation of multimedia contents is still fragmented and that more efforts are required to address it in a comprehensive way.

V. Conclusions and Perspective of Secure WMSNs

Secure wireless multimedia sensor networks provide many interesting applications, but the diffusion of such a technology in real life requires the adoption of an integrated approach that satisfies both security/ privacy and data aggregation/ compression requirements. For this reason, to conclude our analysis and to remark the main open issues in secure WMSNs, herein we summarize driving directions for

future research (Fig. 2). In particular, we identify the following big challenges:

Efficient management of QoS and QoE
At present, such a issue is being addressed by means of cross layer approaches and ad-hoc scheduling algorithms. The standards IEEE 802.11e and 802.15.3 represent the reference solutions, since they are equipped at MAC level with those mechanisms that are required to manage the data flow under different QoS requirements. Moreover, the use of new communication technologies based on cognitive radio networks [8] should be investigated in the future to further improve the management of QoS and QoE. A possible approach should adopt optimization techniques that properly encompass the contrasting requirements of a WMSN to assess the most suitable communication technology, encoding/processing technique, and security policies for a given application context.

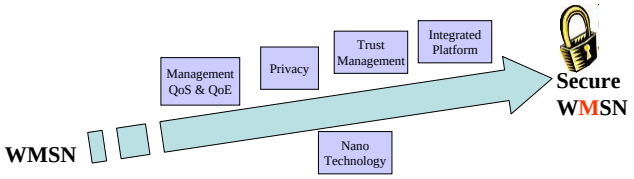

Figure 2: The path to secure WMSN.

Privacy
The privacy solutions described in this paper focus on the specific aspects of data cloaking, secure communication channel, definition of privacy policies. Each solution satisfies only specific requirements for ad-hoc problems, in other words, no single proposal is able to provide a complete privacy solution for WMSNs. The study of integrated theoretical solutions, as well as the development of HW/SW platforms supporting those, represents a great challenge for the scientific community. A possible approach towards the achievement of this goal passes through the definition of a privacy model for WMSNs. The model should support the definition of privacy enabling mechanisms that overcome the limits of WMSN. The model may be used in combination with both data cloaking mechanisms and some other privacy policy based approaches presented in Sec. III.
The model should also support the definition of enforcement schemes that guarantee the correct and automatic application of the privacy policies defined for WMSNs. The enforcement mechanisms indicate the actions that are required to be executed in case behavioral anomalies are identified.

Trust management
A new framework for trust management should be introduced exploiting the capabilities of multimedia sensors (e.g., based on public key digital signature schemes; watermarking schemes). In this context, all the data exchanged among nodes have to be trusted, above all information related to authentication and localization data.
For this reason, research should focus on the development of a flexible framework usable in several application scenarios. The main efforts should be devoted to rethink and adapt schemes already exploited in other distributed systems.

Development of a platform
The platform should allow the integration of existing and upcoming solutions, such as aggregation algorithms, secure localization and so on by considering QoE, security, privacy and technological constraints. The reference platform should be hierarchical. In fact each level of the hierarchy could use different technologies and protocols/algorithms. These research efforts could be a fruitful opportunity to foster new collaborations among different academic and industrial groups around the world. In fact, the aim of developing a solid reference architecture needs expertise coming from many scientific fields and could be the key to go towards new integrated design solutions for secure WMSNs.

Development of nano-technology
This technology [42, 59] should allow to overcome the constrains imposed by the currently available technologies to supply distributed and secure monitoring services based on WMSNs. Upcoming solutions coming from this promising field should be encouraged and timely exploited in order to design next generation monitoring applications.

All these issues should be solved jointly in an integrated approach; only in this manner it is possible to design a real secure WMSN.

REFERENCES

[1] I. F. Akyildiz, T. Melodia, K. R. Chowdhury "A survey on wireless multimedia sensor networks," Computer Networks 51 (2007) 921–960.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," Computer Networks 38 (4) (2002) 393–422.

[3] I. F. Akyildiz, T. Melodia, K. R. Chowdhury "Wireless Multimedia Sensor Networks: Applications and Testbeds ," Proc. of the IEEE, vol. 96 (10), Oct. 2008.

[4] B. H. Walke, S. Mangold, and L. Berlemann, IEEE 802 Wireless Systems. NJ, USA: John Wiley & Sons, 2006.

[5] C. Smith , "3G Wireless Networks, Second Edition," McGraw Hill Communications, 2007.

[6] E. Dahlman, S. Parkvall, J. Skold, P. Beming, "3G Evolution: HSPA and LTE for Mobile Broadband", Academic Press, Oxford, UK, 2007.

[7] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid, Mobile, and Pervasive Computing - chap. 7, Auerbach Publications, CRC Press, 2006.

[8] I. Downes, L. B. Rad, H. Aghajan, "Development of a mote for wireless image sensor networks," in Proc. of COGnitive systems with Interactive Sensors, COGIS, Paris, France, Mar. 2006.

[9] M. Rahimi, R. Baer, O. Iroezi, J. Garcia, J. Warrior, D. Estrin, M. Srivastava, "Cyclops: in situ image sensing and interpretation in wireless sensor networks," in Proc. of SenSys 2005.

[10] Crossbow MICAz, MICA2, Imote, Imote2 Spec., http://www.xbow.com.

[11] Y. Gu, Y. Tian, E. Ekici "Real-time multimedia processing in video sensor networks," Signal Processing: Image Communication 22 (2007) 237–251.

[12] M. H. Yaghmaee, D. Adjeroh, "A Model for Differentiated Service Support in Wireless Multimedia Sensor Networks," in Proc. of ICCCN 2008.

[13] M. Rabbani M., R. Joshi, "An overview of the JPEG 2000 still image compression standard," Signal Processing: Image Communication, Vol. 17, No. 1, Jan. 2002 , pp. 3-48.

[14] C.B. Margi, V. Petkov, K. Obraczka, R. Manduchi, "Characterizing energy consumption in a visual sensor network testbed," in Proc. of IEEE/Create-Net 2006.

[15] W. Feng, B. Code, E. Kaiser, M. Shea, W. Feng, L. Bavoil, "Panoptes: scalable low-power video sensor networking technologies," in Proc. of ACM Multimedia 2003.

[16] M. Chu, J.E. Reich, F. Zhao, "Distributed attention for large video sensor networks," in Proc. of IDSS 2004.

[17] P. Kulkarni, D. Ganesan, P. Shenoy, Q. Lu, "SensEye: a multi-tier camera sensor network," in Proc. of ACM Multimedia 2005.

[18] T. A. Dahlberg, A. Nasipuri, and C. Taylor, "Explorebots: A mobile network experimentation testbed," in Proc. of ACM SIGCOMM Workshop E-WIND 2005.

[19] S. Gurun, Y. Wen, N. Chohan, R. Wolski, C. Krintz, "SimGate: Full-System, Cycle-Close Simulation of the Stargate Sensor Network Intermediate Node," in Proc. of IC-SAMOS 2006.

[20] H. Wang, D. Peng, W. Wang, H. Sharif, H. Chen, "Energy-aware Adpative Watermarking for Real Time Image Delivery in Wireless Sensor Networks" in Proc. of ICC 2008.

[21] T. Lookabaugh, D. C. Sicker "Selective encryption for consumer applications" IEEE Commun. Magazine, vol. 42 (5), pp.124-129, 2004.

[22] W. Wang, D.Peng, H. Wang. H.Sharif, H. Chen, "Energy-Constrained Quality Optimization for secure Image Transmission in Wireless Sensor Networks", Advance in Multimedia, vol. 2007.

[23] E. Magli, M. Mancini, L.Merello, "Low-complexity Video compression for wireless sensor networks" In Proc. of ICME 2003.

[24] R. Wagner, R. Nowak, R. Baranuik, " Distributed image compression for sensor networks using correspondence analysis and super-resolution" in Proc. of ICIP 2003.

[25] C. Tang, C. S. Raghavendra " Compression techniques for wireless sensor networks" in Wireless Sensor Networks, pp. 207-231, Kluwer Academic, Boston, MASS, USA, 2004.

[26] B. Song. O. Bursalioglu, A. K. Roy-Chowdhury, E. Tuncel, " Towards a multi-terminal video compression algorithm using epipolar geometry", in Proc. of IEEE ICASSP 2006.

[27] H. Wu, A.A Abouzeid, " Energy-efficient distributed image compression in resource constrained multihop wireless network" Computer Commun., vol.28, no. 14, pp1658-1668, 2005

[28] V. Lecuire, C. Duran-Faundez, N. Kromeenacker " Energy-Efficient Transmission of Walvet-Based Images in Wireless Sensor Network", EURASIP journal, vol. 2007.

[29] H. Chan, A. Perrig. "Security and Privacy in sensor networks" IEEE Commun. Mag., pp.103-105, 2003.

[30] A. Perrig, J. Stankovic, D.Wagner." Security in wireless sensor networks" Commun. ACM, vol.47, no. 6, pp.53-57, 2004.

[31] A. Perrig, D. Song, R. Canetti, Briscoe, J. Tygar, "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction ". RFC 4082. June 2005.

[32] D. Liu , P. Ning. "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks". In Proc. of NDSS 2003.

[33] D. Liu, P. Ning. "Multi-level μTESLA: Broadcast authentication for distributed sensor networks". ACM Transactions in Embedded Computing Systems, 3(4), 2004.

[34] S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, S. Shenker. "GHT: A geographic hash table for data-centric storage". In Proc. of 1st ACM Int. Workshop on Wireless Sensor Networks and Applications, Sep. 2002.

[35] S. Shenker, S. Ratnasamy, B. Karp, R. Govindan, D. Estrin. "Data-centric storage in sensornets". In Proc. of the First ACM Workshop on Hot Topics in Networks, Oct. 2002.

[36] D. Liu, P.Ning "Security for Wireless Sensor Networks", Springer, 2007.

[37] D. Liu, P. Ning, and W.K. Du. "Attack-resistant location estimation in wireless sensor networks". In Proc of IPSN 2005.

[38] S. Capkun, J.P. Hubaux, "Secure positioning in wireless networks" IEEE J. on Sel. Areas in Commun., vol.24, no. 2: 221-232, 2006.

[39] Z.Liang, W. Shi, " Enforcing cooperative resource sharing in untrusted peer to peer environment.". ACM journal of Mobile Networks and Applications, 10(6): 771-783, 2005.

[40] K.Ren, T.li, Z.Wan, F. Bao, R.H. Deng, K.Kim, "Highly realible trust establishment scheme in ad hoc networks," Computer network, 45, Aug. 2004.

[41] Y. Wang, G. Attebury, B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Commun. Surveys & Tutorials, vol.8, no.2, pp.2-23, Second Quarter 2006.

[42] J. P. M. She and J. T. W. Yeow, "Nanotechnology-Enabled Wireless Sensor Networks: From a Device Perspective," IEEE Sensors Journal, Vol. 6 (5) Oct. 2006.

[43] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald. Privacy-aware location sensor networks. In 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX), 2003.

[44] H. Chan and A. Perrig. Security and privacy in sensor networks. IEEE Computer Magazine, pages 103105, 2003 2003

[45] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. Spins: security protocols for sensor networks. Wireless Networking, 8(5):521534, 2002.

[46] M. Gruteser and D. Grunwald. A methodological assessment of location privacy risks in wireless hotspot networks. In First International Conference on Security in Pervasive Computing, 2003.

[47] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The cricket locationsupport system. In Proc. of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MOBICOM), August 2000.

[48] A. Smailagic, D. P. Siewiorek, J. Anhalt, and Y. Wang, D. Kogan. Location sensing and privacy in a context aware computing environment. In Pervasive Computing, 2001.

[49] D. Molnar and D. Wagner. Privacy and security in library rfid : Issues, practices, and architectures. In ACM CCS, 2004

[50] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J. Tang.Framework for security and privacy in automotive telematics. In 2nd ACM International Worksphop on Mobile Commerce, 2000.

[51] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31.

[52] http://www.hipaa.org

[53] http://www.glba.org

[54] Q. Ni, A. Trombetta, E. Bertino, and J. Lobo. Privacy-aware role-based access control. In Proc. of ACM Symp. on Access Control Methods And Technologies (SACMAT07), 2007.

[55] M. Langheinrich. A privacy awareness system for ubiquitous computing environments. In 4th Int. Conf. on Ubiquitous Computing, 2002.

[56] E. Snekkenes. Concepts for personal location privacy policies. In Proc. of the 3rdACM Conf. on Electronic Commerce, 2001.

[57] J. Al-Muhtadi, R. Campbell, A. Kapadia, M. D. Mickunas, and S. Yi. Routing through the mist: privacy preserving communication in ubiquitous computing environments. In Proc. of IEEE Int. Conf. on Distributed Computing systems (ICDS),Vienna(Austria), 2002.

[58] P. Samarati, and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization

and suppression. Technical Report SRI-CSL-98-04, Computer Science Laboratory, SRI International, 1998.

[59] I.F. Akyildiz, F.Brunetti, and C.Blazquez,, "NanoNetworking: A New Communication Paradigm", Computer Networks Journal, (Elsevier), June 2008.

[60] S. Misra, M. Reisslein, and X.Guoliang , "A survey of multimedia streaming in wireless sensor networks," IEEE Communications Surveys & Tutorials, Vol. 10(4), Fourth Quarter 2008.

[61] W. Wang, D.Peng, H.Wang,and H. Sharif "A cross layer resource allocation scheme for secure image delivery in wireless sensor networks," in Proc. of International conference on Wireless communications and mobile computing IWCMC 2007, pp. 152-157.

[62] W..Zeng, S.Lei,"Efficient frequency domain selective scrambling of digital video," IEEE Trans. Multimedia, vol. 5, no. 1, pp.118-129, Mar. 2003

[63] M.Kankanhalli, T.Guan, "Compressed domain scrambler/descrambler for digital video," IEEE Trans. Consum. Electron., vol. 48, no. 2, pp.356-365, May 2002

[64] C.Wu, C.Kuo, "Design of integrated multimedia compression and encryption systems," IEEE Trans. Multimedia, vol. 7, no. 5, pp.828 - 839, Oct. 2005

[65] L.Tang, "Methods for encrypting and decrypting MPEG video data efficiently," in Proc. 4th Int. Conf. ACM Multimedia, pp.219-229, Nov. 1996

[66] M.Grangetto, E.Magli, G.Olmo, "Multimedia Selective Encryption by Means of Randomized Arithmetic Coding,"IEEE Trans. Multimedia, vol. 8, no. 5, pp.905-917, Oct. 2006

[67] Hong Luo, Yonghe Liu, and Sajal K. Das, "Distributed Algorithm for En Route Aggregation Decision in Wireless Sensor Networks," IEEE Trans. on Mobile Computing , Vol. 8, No. 1, Jan. 2009.

[68] Hong Luo Luo, J. Liu, Y. Das, S.K., "Adaptive Data Fusion for Energy Efficient Routing in Wireless Sensor Networks," IEEE Trans. on Computers, Vol. 55, No. 10, Oct. 2006.

[69] R. B. Abidi, R. N. Aragam, Y. YAO, and M. A. ABIDI, "Survey and Analysis of Multimodal Sensor Planning and Integration for Wide Area Surveillance," ACM Computing Surveys, Vol. 41, No. 1, Article 7, Dec. 2008.

[70] I. Politis, M. Tsagkaropoulos, andS. Kotsopoulos, "Optimizing Video Transmission over Wireless Multimedia Sensor Networks," in Proc. of IEEE GLOBECOM 2008.

[71] I. Politis, M.Tsagkaropoulos, T. Pliakas, and T.Dagiuklas, "Distortion Optimized Packet Scheduling and Prioritization of Multiple Video Streams over 802.11e Networks," Advances in Multimedia, Vol. 2007 (2007), Hindawi Publishing Corporation.

[72] L.W. Chew, L. M. Ang, K. P. Seng, "Survey of Image Compression Algorithms in Wireless Sensor Networks", in Proc. of Int. Symp. on Information Technology (ITSim 2008), Aug. 2008.

[73] A. Said, and W. A. Pearlman, "A new fast and efficient image codec based on set partitioning in hierarchical trees," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 6, No. 3, Jun. 1996.

[74] M. Guerrero-Zapata, R. Zilan, J. M. Barcelo-Ordinas, K. Bicakci, and B. Tavli, The Future of Security in Wireless Multimedia Sensor Networks: a position paper, accepted by the Special Issue "Secure Multimedia Services" in Telecommunications System Journal (Springer), 2009

[75] G. Gaubatz, J. P. Kaps, and B. Sunar, "Public key cryptography in sensor netwroks – revisited," Lecture Notes in Computer Science, vol. 3313, pp. 2-18, Springer, 2004.

[76] G. Gaubatz, J. P. Kaps, E. Ozturk, and B. Sunar, "State of the art in ultra-low power public key," in Proc. of The 2nd IEEE Int. Workshop on Pervasive Computing and Communication Security. 2005.

[77] R. Watro, D. Kong, S. F. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: securing sensor networks with public key technology," in Proc. of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 59–64. 2004.

[78] H. Goto, Y. Hasegawa, and M. Tanaka, "Efficient Scheduling Focusing on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.

[79] B. P. L. Lo, J. L. Wang, and G.-Z. Yang, BFrom imaging networks to behavior profiling: Ubiquitous sensing for managed homecare of the elderly,[in Adjunct Proc. Int.Conf. Pervasive Comput., Munich, Germany,May 2005, pp. 101–104.

[80] D. A. Fidaleo, H.-A. Nguyen, and M. Trivedi,BThe networked sensor tapestry (NeST): A privacy enhanced software architecture for interactive analysis of data in video-sensor networks,[in Proc. ACM Int. Workshop Video Surveill. Sensor Netw., New York, Oct. 2004, pp. 46–53.

[81] D. Kundur and W. Luh and U. N. Okorafor and T. Zourntos Security and Privacy for Distributed Multimedia Sensor Networks Proceedings of the {IEEE} Special Issue on Recent Advances in Distributed Multimedia Communications,January 2008, 96(1),pp112--130}

[82] J. Wickramasuriya, M. Datt, S. Mehrotra, and N. Venkatasubramanian, B Privacy protecting data collection in media spaces, in Proc. ACM Int. Conf. Multimedia, New York, Oct. 2004,pp. 48–55.

[83] H. Yamamoto, BRate-distortion theory for the Shannon cipher system,[IEEE Trans. Inf. Theory, vol. 43, pp. 827–835, May 1997.

[84] M. Naor and A. Shamir, BVisual cryptography,[in Proc. Adv. Cryptol.VEUROCRYPT '94: Workshop TheoryApplicat. Crypto. Tech., 1995, pp. 1–12

[85] Y.Xi, L. Schwiebert, and W.Shi, W.: Preserving source location privacy in monitoring-based wireless sensor networks. Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International pp. 8 pp.– (2006)

[86] Y.Yang, M. Shao, and S.Zhu, B.Urgaonkar., and G.Cao,.: 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. ACM, New York, NY, USA (2008).

[87] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of the First International Conference on Mobile Systems, Applications, and Services (MobiSys).USENIX, 2003.

[88] SSL,RFC5246 http://tools.ietf.org/html/rfc5246

[89] C. Castelluccia, "Securing Very Dynamic Groups and Data Aggregation in Wireless Sensor Networks," IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems, MASS 2007.