Wireless Multimedia Sensor Networks Applications and Security Challenges

Bambang Harjito[1,2]
[1]Digital Ecosystem and Business Intelligence Institute
Curtin University of Technology, Perth, Western Australia
harjito.bambang@postgrad.curtin.edu.au
[2]Computer Science Department, Faculty of Mathematics and Natural Science
Sebelas Maret University, Surakarta, Indonesia

Song Han[1],
[1]Digital Ecosystem and Business Intelligence Institute
Curtin University of Technology, Perth, Western Australia
Song.Han@cbs.curtin.edu.au

Abstract— **The emergence of low-cost and mature technologies in wireless communication, visual sensor devices, and digital signal processing facilitate of wireless multimedia sensor networks (WMSNs). Like sensor networks which respond to sensory information such as humidity and temperature, WMSN interconnects autonomous devices for capturing and processing video and audio sensory information. WMSNs will enable new applications such as multimedia surveillance, traffic enforcement and control systems, advanced health care delivery, structural health monitoring, and industrial process control. Due to WMSNs have some novel features which stem the fact that some of the sensor node will have video cameras and higher computation capabilities. Consequently, the WMSNs bring new security of challenges as well as well as new opportunities. This paper presents WMSNs application and security challenges.**

Keywords-component; Security, Wireless Multimedia Sensor Networks.

I. INTRODUCTION

The availability of multimedia devices such as a small microphones and low-cost complementary metal-oxide semiconductor (CMOS) has fostered the development of wireless multimedia sensor network (WMSN). These multimedia devices can capture multimedia content such as scalar data, stream audio and video from the environment. Thereby a WMSN will have the ability to transmit and to receive multimedia information such as monitoring data, image, voice, and stream video. Since the ability to retrieve multimedia information so the WMSN will also be able to store, process in real time, correlate and fuse multimedia information from different sources. Thus, WMSNs are composed of numerous type multimedia sensors which exchange sensed multimedia data with sink by using wireless channel [1]. WMSNs will not only change enhance existing sensor applications such as tracking, and environment monitoring, but they will also enable several new applications. For example they range over systems supporting telemedicine to modern military.

In WMSNs, data harvested from the environmental is not only a scalar nature which is obtained from various internal sensor such as temperature, light, humidity, pressure, and acoustic sensor but also from multimedia data such as digital images, video and audio form [2]. Therefore the main sensor in WMSN is the imager. The visual data which is handled puts severe constraints on a sensor network. Collection, processing, and visual data dissemination is a processing intensive and high bandwidth demanding operation. WMSNs have some novel features which stem the fact that some of the sensor node will have video cameras and higher computation capabilities. Consequently, the WMSNs bring new security of challenges as well as well as some new opportunities.

The paper is structured as follows: Section 2 explains WMSNs components, Section 3. present review all the aspects of WMSNs architecture Section 4 describes WMSNs application, Section 5 describe security and challenges , Section 6 we examine a number of security design and finally we have concluded the paper in section 7.

II. WIRELESS MULTIMEDIA SENSOR NETWORK HARDWARE COMPONENTS

In this section we discuss hardware components of WMSN specially in the multimedia sensor node. In [2], it states that an enabling hardware platforms multimedia sensor hardware has divided in two categories depending on it's resolution. Low-resolution imaging motes and Medium-resolution imaging motes based on the Star gate platform [2]

- The low-resolution imaging motes.

The technology of CMOS imaging sensor that capture and process an optical image allows integrating a lens, an image sensor and image processing algorithms, including image stabilization and image compression, on a single chip. Existing CMOS images is still developed. In [3] introduced a Cyclops which consist of an image CMOS Agilent ADCM-1700 CIF camera), a complex programmable logic device, an external SRAM and an external flash. The objective of this Cyclops is to fill a gap between computational devices and CMOS cameras. The design of an integrated mote with wireless sensor networks is explained in [4]. This design is based on an adequate processing power and memory size for application. Here a new image mote is based on an ARM7 32-bit CPU clocked at 48 MHz, with external FRAM or

978-0-7695-4236-2/10 $26.00 © 2010 IEEE
DOI 10.1109/BWCCA.2010.182

Flash memory, 802.15.4 compliant Chipcon CC2420 radio and low-resolution 30 x 30 pixel optical sensors.

- Medium-resolution imaging motes based on the Star gate platform

The stargate board [5] was produced by Crossbow and designed by Intel. This stargate board, based on Intel's PXA-255 Xscale 400MHz RISC processor, is a high performance processing platform designed for sensor, robotic and sensor networks applications. It also 32 Mbyte of flash memory, 64 Mbyte of SDRAM and on-board connector Crossbow's MICAz or MICA2. The another prototype has developed by Intel such as Imote and Imote2.

Suh et al [6] introduced a novel solution for improving IEEE 802.15.4 performance with the adaptive active duration via two data traffic indication schemes, designed and implemented a real sensor platform and its camera module for testbed experiments. The development of a low cost, low power WSN hardware platform named *TelG* embedded with an operating system called *WiseOS*, system software, and also a simple best effort JPEG images transmission over the network [7]

There has been a lot of work to develop in this field however the growing technology is still not mature and still need several technical challenges.

III. WIRELESS MULTIMEDIA SENSOR NETWORK ARCHITECTURE

In this section we survey the network architecture for WMSN in[1, 2, 8, 9]. The basic architecture of WMSN. It can be shown in Fig.1

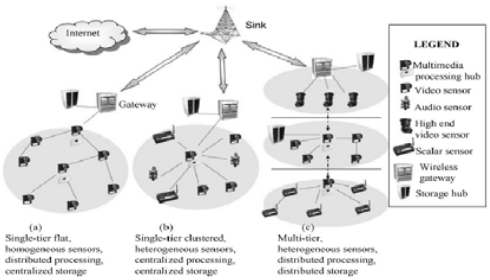
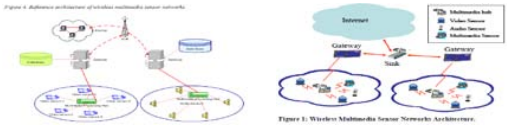


Fig. 1 Architecture of WMSN [2]

There are three model depending on the targeting application nature i.e., the first 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, 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 and 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.

Elhadi et al [8] was described typical characteristics of WMSNs and introduced a reference architecture for WMSNs similar to [2]. It can be show in Fig. 2.a. Grieco et al [1] introduces an architecture of WMSN. It is composed of numerous multimedia sensors that exchange sensed data with sinks using a wireless channel. It can be seen in Fig.2.b.



(a) (b)

Fig. 2 Architecture of WMSN [8] and [1]

There have been many designs to develop an architecture for WMSNs. The design is still similar to [2].

IV. WIRELESS MULTIMEDIA SENSOR NETWORK APPLICATIONS

The characteristic of a WMSN diverge consistently from traditional network paradigms, such as the internet and even from the WSNs. The most potential applications of WMSNs require the sensor networks paradigm to be rethought to provide mechanisms to delivery multimedia contents with the predetermined level of Quality of Service (QoS). WMSNs will enable several new applications.

- *Surveillance:* WMSNs are used currently in surveillance which need streaming multimedia content, advanced signal and high bandwidth. Such as Audio and video sensors will be used to complement and enhance existing surveillance systems against crime attack [10].
- *Traffic monitoring and Enforcement* : WMSNs are low cost, easy of deployment and ease for reconfiguring routes when deployment in the specific location such as in big cities of highways. They will be possible to monitor car traffic and to service that offer traffic routing advice to avoid congestion [11].
- *Personal and Health care* : WMSNs, incorporated with some telemedicine devices, can be used to remotely monitor the patient's body temperature, blood and breathing activity etc. They can be studied the behavior of elderly people as means to identify the causes of illnesses that affect them such as dementia [12].
- *Gaming*: WMSNs will find applications in the future prototypes that enhance the effect on the game player. Such as virtual reality games that assimilate touch and sight input, of user as part of the player response [13].
- *Environmental and industrial* : Array of video sensors are used by Oceanographer to determine the evolution of sandbars using image processing

techniques [14] and multimedia content such as imaging, temperature, or pressure can be used for time-critical industrial process control.

V. SECURITY CHALLENGES IN WIRELESS MULTIMEDIA SENSOR NETWORKS

In this section we discuss security and challenge for WMSNs. In WMSN, we know that data harvested from the target area is not only scalar nature such as humidity, temperature, light, pressure , seismic but also more complex such as image and streaming video. Therefore the energy dissipation in multimedia sensor nodes is dominated by the computation energy rather than the communication energy.

Manel et al [9] provided a survey and analysis of the different security issues that will have to take into account in the design of WMSNs platforms and protocol. Grieco et al [1] summarize the main findings on secure WMSNs and forecasts future perspectives of such a technology. Here we address security according to these into four categories.

1. Efficient management of Quality of Experience (QoE) and Quality of Service (QoS).
   The requirement of the multimedia monitoring applications state new problems which wireless communication and infrastructures of processing have to solve to assure the QoE. Such as the problem of the limited power resources and computational capabilities [15, 16] and the problem of computational complexity of compression are considered. In addition the problem of aggregation, distributed processing, the overload to manage privacy/security and QoS are also considered.
2. Privacy
   In WMSNs collect and handle a great amount of data of different nature, which may provide some kind of information on individuals in both a direct or indirect form. The kind of information may specify explicit information on individuals. Therefore, under some circumstances, data may be used to violate the privacy of individuals. Privacy is a key requirement for numerous application scenarios of WMSNs. The privacy solutions, such as secure data cloaking [17], secure communication channel [18, 19] and definition of privacy policies [20-22] are not enough to provide a complete privacy solution for WMSNs. Due to each solution satisfies only specific requirements ad-hoc problems.
3. Authentication and Node localization
   In WSNs communications, Han et al [23] describe a taxonomy of attacks on WSNs. The taxonomy consists of six attacks i.e., communication attacks, attacks against privacy, sensor node targeted attacks, power consumption attacks, policy attacks and cryptology attacks on key management. In communication attacks, Eavesdropping can easily inject messages, so the receiver needs to make sure that the data used any decision–making process originates from the correct source. Data authentication prevents unauthorized parties from participating in the networks and legitimate nodes should be able to detect messages from authorized nodes and reject them. The authenticity of these data and commands is a critical requirement for the correct behaviour of a WMSN [1]. The problem of the authentication is strictly related to the secure node localization issue [23]. Authentication can be used to ensure reliable information. Because of the distributed nature of WMSNs, 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.
4. Development of Platform.
   The integration of existing and upcoming solutions, such as aggregation algorithms, compression technique, secure localization, authentication mechanisms, should be allowed by the platform such as sensEye [24-26]. Here, the platform considers QoE, security, privacy and technological constraints. The reference platform should be hierarchical. Each level of the hierarchical could be use different protocol/algorithm and technologies. Research efforts should be a opportunity to foster new collaborations between different academic and industrial group.

VI. DESIGN CHALLENGES FOR SECURITY SCHEMES WIRELESS MULTIMEDIA SENSOR NETWORKS

In this section, we give security design challenge for WMSNs. Sensor nodes are often deployed in unattended and even harsh environments. They may suffer from many kinds of attacks. Wireless channels are low-cost and unreliable. The transmission of data packets may be delay or may not reach its destination. Indeed, security challenges and opportunities in WMSNs stem from these characteristics [9]. Here we examine a number of security design challenges:

- **Unattended deployment environments**:

Sensor nodes often deployed in a large unattended area. An attacker may compromise one or a number of sensor nodes without being noticed. As a consequence, no solution is specifically deployed for WMSNs. Hence, new approaches exploiting the characteristics of multimedia nodes should be developed [1]. There are many papers that explain to deploy sensor node. Such as designing multimedia sensor networks to support volcanic studies requires addressing the high data rates and high data fidelity and sparse array with high spatial separation between nodes [27], however in this paper is not described the security of the sensor node. Tzu et al [28] explains

a procedure of deployment for a wireless sensor network. It is addressed to guide users to complete the deployment tasks systematically and Younis et al [29] survey on the current state of the research on optimized node placement in WSNs. Both of them is only used to deploy WSN and is not concerned to secure of the sensor node.

- **Data Privacy**:

Privacy issues are of concern in WSNs, 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 [18, 19] may be crucial for WMSNs. Attacks versus privacy which exploit these vulnerabilities can be categories into distinct macro-types of techniques: Eavesdropping and Masquerading. The design of privacy protecting mechanisms is a challenging problem for the intrinsic characteristic of WMSNs.

Gruteser et al [30] proposed a methodology for identifying, assessing and comparing location privacy risk in mobile computing technologies. However, this method cannot be used for design securing in WMSNs. The source location privacy problem is studied in [31] under the assumption of one single source during a specific period. However, this method is not specifically defined for WMSNs.

Yi et al [32] propose a Proxy based Filtering Scheme (PFS) and a Tree-based Filtering Scheme (TFS), which are simple yet efficient event source unobservability preserving solutions for sensor networks. However these methods are not suitable for securing in WMSNs.

- **Data authentication**:

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 [33] are required to guarantee the correctness and the confidentiality of data. Moreover, due to the high number of sensor nodes, such systems could contain control units that broadcast commands and data to the nodes. Hence, the authenticity of these data and commands is a critical requirement for the correct behaviour of WMSNs. Data authentication guarantees and ensures that raw data are received at the aggregators at the same time as they are being sensed. Zhang et al [34] proposed a watermark statistical approach for data authentication in WSN which provides inherent support for in-network processing. The data authentication is only work from sensor nodes to the data sink. However secure data authentication is not explained from the sink to the sensor node. In the literature [35, 36] provide authentication algorithm for data authentication however this algorithm is not adequately satisfy the quality of service requirements of multimedia signals.

- **Multimedia in-network processing :**

Multimedia in networks processing is one of the factors influencing the design of WMSNs. WMSNs allow algorithm of processing of multimedia content from the environment. A new architecture for collaborative, distributed, and resource-constrained processing is required. This architecture allows for filtering and extraction of semantically relevant information at the edge of the sensor network. Nath et al [37] introduces IrisNet which uses application-specific filtering of sensor feeds at the source and reduces the bandwidth consumed, since instead of transferring raw data, IrisNet sends only a potentially small amount of processed data. Stockdon, et al [38] introduce distributed filtering technique that can create a time-elapsed image in video security application. Both of them is concerned to specific filtering of sensor. However they do not concerned for securing in networks processing in WMSNs.

VII. CONCLUSION

In this paper, we aims to address the problem of secure and challenges in WMSNs . We have also discussed the existence hardware component and surveyed the network architecture for WMSNs. The application of WMSNs is explained. This paper is also figure out a number of security challenges. Based on this paper, we will next to try to design a conceptual frame work for securing in WMSNs.

REFERENCESS

1. Grieco, L.A., Boggia, G, Sicari, S, Colombo, P. *Secure Wireless Multimedia Sensor Networks: A Survey*. in *Mobile Ubiquitous Computing, Systems, Services and Technologies, 2009. UBICOMM '09. Third International Conference on*. 2009.
2. Akyildiz, I.F., T. Melodia, and K.R. Chowdhury, *A survey on wireless multimedia sensor networks.* Computer Networks, 2007. **51**(4): p. 921-960.
3. Mohammad, R.R., Baer Obimdinachi, I. Iroezi Juan, C. Garcia Jay, Warrior Deborah, Estrin Mani, Srivastava, *Cyclops: in situ image sensing and interpretation in wireless sensor networks*, in *Proceedings of the 3rd international conference on Embedded networked sensor systems*. 2005, ACM: San Diego, California, USA.
4. Ian Dowes, L.B., Hmid Aghajan *Development of a Mote for Wireless Sensor Networks.* in. Proceeding of Cognitive System and Interactive Sensor(COGIS) Paris, , 2006.
5. Crossbow Mote Specifications, h.w.x.c., http://www.xbow.com, 3th July 2010
6. Suh, C.M., Zeeshan Hameed Ko, Young-Bae, *Design and implementation of enhanced IEEE 802.15.4 for supporting multimedia service in Wireless Sensor Networks.* Computer Networks, 2008. **52**(13): p. 2568-2581.
7. Abdul Hadi Fikri Bin Abdul Hamid, R.A.R., Norsheila Fisal, S. K. S. Yusof, S. H. S. Ariffin Liza Latiff, *Development of IEEE802.15.4 based Wireless Sensor Network Platform for Image Transmission.* International Journal of Engineering & Technology IJET 2009. **9**(10): p. 7.
8. Elhadi Shakshuki, X.X., Haroon Malik *An Introduction to Wireless Multimedia Sensor Networks.* 2009: p. 16.

9. Manel Guerrero Zapata, R.Z., Jos´e M, Barcel´o-Ordinas, Kemal Bicakci, Bulent Tavli, *The Future of Security in Wireless Multimedia Sensor Networks.* 2009.
10. Dan, L.W., K. D. Yu Hen, Hu Sayeed, A. M., *Detection, classification, and tracking of targets.* Signal Processing Magazine, IEEE, 2002. **19**(2): p. 17-29.
11. Arth, C.B., H. Leistner, C. *TRICam - An Embedded Platform for Remote Traffic Surveillance*. in *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW '06. Conference on*. 2006.
12. Reeves, A.A., *Remote monitoring of patients suffering from early symptoms of dementia.* in Proc. Int. Workshop Wearable Implantable Body Sensor Networks: p. London, U.K., Apr. 2005.
13. Mauricio, C., et al., *The multimedia challenges raised by pervasive games*, in *Proceedings of the 13th annual ACM international conference on Multimedia*. 2005, ACM: Hilton, Singapore.
14. Rob, H., S. John, and O.-H. Tuba, *Applying Video Sensor Networks to Nearshore Environment Monitoring.* IEEE Pervasive Computing, 2003. **2**(4): p. 14-21.
15. I. Downes, L.B.R., H. Aghajan, *Development of a mote for wireless image sensor networks.* in Proc. of COGnitive systems with Interactive Sensors, COGIS Paris, France: p. Mar. 2006.
16. Margi, C.B., et al. *Characterizing energy consumption in a visual sensor network testbed*. in *Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006. 2nd International Conference on*. 2006.
17. Kundur, D.L., W. Okorafor, U. N. Zourntos, T, *Security and Privacy for Distributed Multimedia Sensor Networks.* Proceedings of the IEEE, 2008. **96**(1): p. 112-130.
18. Douglas, A.F., N. Hoang-Anh, and T. Mohan, *The networked sensor tapestry (NeST): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks*, in *Proceedings of the ACM 2nd international workshop on Video surveillance \& sensor networks*. 2004, ACM: New York, NY, USA.
19. Adrian, P.R., Szewczyk J. D. Tygar Victor, Wen David, E. Culler, *SPINS: security protocols for sensor networks.* Wirel. Netw., 2002. **8**(5): p. 521-534.
20. Sastry, D.M., Gruteser Xuan, Liu Paul, Moskowitz Ronald, Perez Moninder, SinghJung-Mu, Tang, *Framework for security and privacy in automotive telematics*, in *Proceedings of the 2nd international workshop on Mobile commerce*. 2002, ACM: Atlanta, Georgia, USA.
21. Qun, N., Alberto, Trombetta, Elisa, Bertino, Jorge, Lobo, *Privacy-aware role based access control*, in *Proceedings of the 12th ACM symposium on Access control models and technologies*. 2007, ACM: Sophia Antipolis, France.
22. Mark, M.J., rg, Schwenk, *Security model and framework for information aggregation in sensor networks.* ACM Trans. Sen. Netw., 2009. **5**(2): p. 1-28.
23. Han S , L.G., Chang E , Tharam D, *Taxonomy of Attacks on Wireless Sensor Networks.* Proceedings of the First European Conference on Computer Network Defence School of Computing, University of Glamorgan Wales, UK, 2006.
24. Wu-Chi, F.E., Kaiser Wu Chang, Feng Mikael Le, Baillif, *Panoptes: scalable low-power video sensor networking technologies.* ACM Trans. Multimedia Comput. Commun. Appl., 2005. **1**(2): p. 151-167.
25. Teresa, A.D.A., Nasipuri Craig, Taylor, *Explorebots: a mobile network experimentation testbed*, in *Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*. 2005, ACM: Philadelphia, Pennsylvania, USA.
26. Purushottam, K.D., Ganesan Prashant, Shenoy Qifeng, Lu, *SensEye: a multi-tier camera sensor network*, in *Proceedings of the 13th annual ACM international conference on Multimedia*. 2005, ACM: Hilton, Singapore.
27. Geoffrey, W.-A.K., Lorincz Matt, Welsh Omar, Marcillo Jeff, Johnson Mario, Ruiz Jonathan, Lees, *Deploying a Wireless Sensor Network on an Active Volcano.* IEEE Internet Computing, 2006. **10**(2): p. 18-25.
28. Tzu-Che Huang, H.-R.L.a.C.-H.K., *A deployment procedure for wireless sensor networks.* Networks and Multimedia Institute, Institute for Information Industry., 2007.
29. Younis, M.A., Kemal, *Strategies and techniques for node placement in wireless sensor networks: A survey.* Ad Hoc Networks, 2008. **6**(4): p. 621-655.
30. Marco Gruteser, D.G., *A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks.* In First International Conference on Security in Pervasive Computing, 2003.
31. Y.Xi, L.S., and W.Shi, W, *Preserving source location privacy in monitoring-based wireless sensor networks.* Parallel and Distributed Processing Symposium 2006. IPDPS 2006. 20th International 2006: p. 8.
32. Yi, Y.M., Shao Sencun, Zhu Bhuvan, Urgaonkar Guohong, Cao, *Towards event source unobservability with minimum network traffic in sensor networks*, in *Proceedings of the first ACM conference on Wireless network security*. 2008, ACM: Alexandria, VA, USA.
33. Honggang, W.D., Peng Wei, Wang Sharif, H. Hsiao-Hwa, Chen. *Energy-Aware Adaptive Watermarking for Real-Time Image Delivery in Wireless Sensor Networks*. in *Communications, 2008. ICC '08. IEEE International Conference on*. 2008.
34. Zhang, W.L., Yonghe Das, Sajal K. De, Pradip, *Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach.* Pervasive and Mobile Computing, 2008. **4**(5): p. 658-680.
35. Liu, D. and P. Ning, *Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks*. 2002, North Carolina State University at Raleigh.
36. Liu, D. and P. Ning, *Multi-Level microTESLA: A Broadcast Authentication System for Distributed Sensor Networks*. 2003, North Carolina State University at Raleigh.
37. S. Nath, Y.K., P.B. Gibbons, B. Karp, S. Seshan, *A distributed filtering architecture for multimedia sensors,*. Intel Research Technical Report IRP-TR-04-16, agustus, 2004.
38. H. Stockdon, R.H., *Estimation of wave phase speed and nearshore bathymetry from video imagery.* J. Geophys Res. 105 (C9) 22 ,015–22,033, 2000.