Security Mechanisms for Wireless Multimedia Sensor Networks: A Survey

Angel Dimoski, Zoran Kotevski, Nikola Rendevski

"St. Kliment Ohridski" University – Bitola,
Faculty of information and communication technologies
Partizanska bb, 7000 Bitola, Macedonia
{zoran.kotevski, nikola.rendevski, angel.dimoski}@fikt.edu.mk

Abstract. The technological advances of microelectromechanical (MEMS) systems created novel developmental horizons for powerful sensor-based distributed intelligent systems, capable of retrieving various multimedia content such video and audio streams, still images and scalar sensor data from the physical environment. This wirelessly networked paradigm is called Wireless Multimedia Sensor Networks (WMSNs). WMSNs are designed for both real-time mission-critical applications, which demand strict quality of service (QoS) requirements, such low delay, high throughput and reliability, as well as non-real-time applications which require medium bandwidth and allow certain loss tolerance. In both application scenarios, a concern of great importance nowadays is the data security of WMSNs. As the number of application and usage models rely on the concept of WMSNs, significant research and development attention is dedicated to various mechanisms towards providing privacy and security of such systems. Besides the well-known methods based on cryptography algorithms for data protection, different security challenges are required for each encryption techniques, mostly as a result on constraints of a different nature. At this context, this work presents a survey on the security mechanisms in WMSNs and their performance, complexity and suitability for implementation in WMSNs.

Keywords: wireless multimedia sensor networks, security, QoS, multimedia encryption.

1. Introduction

WMSNs are networks built from wirelessly connected smart devices capable of capturing video and audio streams, still images, and scalar sensor data in real-time and non-real-time application scenarios. WMSNs development coexist with the recent developmental trends of the next-generation network paradigms, such Internet of Things (IoT), Cyber Physical Systems (CPS), Industry 4.0 and Tactile Internet (TI) as 5G-enabled communication technologies, changing the way of how information may be generated and transmitted. In such developmental roadmap, the massive production of multi-sensor networked devices, capable to produce and distribute larger and high quality multimedia content is highly expected. Sensor-based systems could span a wide range of application areas, including scientific research, military, disaster recovery and rescue, healthcare, industry and robotics, environmental monitoring, smart homes etc. [1]. In [2], the WMSNs applications are classified in five categories: Surveillance, Traffic Monitoring, Personal and Health Care, Gaming and Environment and Industry. Those applications transmit different types of multimedia data. In some cases the data is transmitted during short periods of time (images), but others require transmission of large amounts of multimedia content in real time (streaming). Considering the wireless transmission in well-known and crowded frequency bands, the risk of unauthorized eavesdropping and changing the data during transmission, open real security challenges for WMSNs [3]. Furthermore, Denial of Service (DoS) attacks are particularly devastating for resource-constrained wireless sensor nodes and also demands appropriate security measures. Among the available security protection mechanisms for WMSN, the conventional cryptography techniques are effective and can provide confidentiality, integrity and authenticity to sensed data and sensor nodes. Cryptography is a science area which provides techniques for protecting data with transformation of original unprotected data into unreadable data structure, which can only be read by an appropriate recipient. Cryptography includes two processes, encryption and decryption, where the transmission of the data decryption key is ciphered as well. Different multimedia services have different QoS and encryption demands [4]. Hence, this paper provides a survey and analysis of the security challenges in the design of WMSN platforms and protocols. In Section 2, we present the existing security challenges in WMSNs context. Cryptography algorithms are surveyed and discussed in Section 3, while the encryption mechanisms for multimedia streaming are presented in section 4. Section 5 concludes the paper with summary of the contribution.

2. Security in Wireless Multimedia Sensor Networks

As the radio waves are considered as transmission media in WMSN, it is well known that such systems are significantly more vulnerable to attacks than the wired networks [3]. The increased use of sensing devices with communication capabilities and limited processing power, produces security threats that can harm the applications in many ways, as the resource-constrained nature of sensor nodes plays a central role in the implementation of security mechanisms. According to [6], where the security requirements are discussed, and most WMSNs applications are affected by at least one of the following: authenticity, availability, confidentiality, data freshness, integrity and localization. Authentication mechanisms, secure localization algorithms, trust management, privacy aspects, secure compression and aggregation algorithms are presented in [8]. Besides the existing security mechanisms and well known technologies widely implemented in other networking technologies, one question naturally rises: what is the exact justification of security analyses of WMSNs as a result of its characteristic architecture and types of attacks specific for this network paradigm? There are several types of attacks in WMSN, which can compromise security requirements. Some of the attacks can be avoided or minimized, but some of them may not be easily avoided such as intrusion attacks and DoS attacks. Attackers are looking for vulnerabilities, which could be found in some communication layers, and they can perform eavesdropping on the transmission, altering confidential data or prejudicing the network operation with the insertion of malicious information. Security attacks in WMSN may be of four different types: interruption, interception, modification and fabrication. Differences between them are: interruption attacks compromise availability; interception compromise confidentiality; modification prejudices integrity; and fabrication impairs authentication [9]. In such a way, security defenses are often required, and there are many ways to protect wireless multimedia sensor networks.

In a wireless sensor network which supports multimedia streaming applications, denial of service (DoS) and service disruptions can become severe problems. An adversary can corrupt or inject false multimedia packets, and these packets may be forwarded all the way to the base station where they are found to be unusable. This sensor nodes would be drained much faster of battery energy [7]. It is expected that DoS will be the main attack to be worried about in most of the WMSN. DoS attacks represent quite complex problems, since they can be performed in many different ways, and against any of the different communication layers. In [10] different DoS attacks are presented (Physical attacks, Tampering attacks, Jamming attacks, Collision attacks, MAC protocol attacks, Routing Protocol attacks, Transport layer protocols attacks and Intrusion attacks. With Eavesdropping attacks the wireless communication channel and the 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 provides data retrieving 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 in the communications. For eavesdropping and masquerading attacks there are three different types of solutions: anonymity mechanisms based on data cloaking, privacy aware mechanisms based on secure communication channels and privacy policy based approaches [8].

Security defenses may be focused on the network or on the data. When protecting the network, secure protocols may be used to avoid attacks, as denial of service, man-in-the-middle and general packet redirection. But, concerning the data the most effective approach is cryptography, which is the basic defense mechanism in wireless sensor networks that directly protects the data. Cryptography is a set of techniques for transforming original information into a set of unreadable data, allowing it to be read only by the correct recipients [6, 11, 12]. Because of the constrains that are inherent to wireless sensor networks, especially the ones with high computing power and communication overhead, traditional cryptography may not be feasible for WMSN, and therefore optimized cryptography is employed. Cryptography provides authenticity, confidentiality and integrity for wireless multimedia sensor networks. The use of cryptography keys provides authentication of source nodes, where such keys would be required to recover the original data and confidentiality assured as well. Furthermore, if the original information cannot be accessed, it cannot be adulterated, which adds to the provision of integrity. Authors in [7] concluded that all existing multimedia encryption schemes are based on three mechanisms: position permutation, value transformation and combination. In [5], security is divided in four categories: Efficient management of Quality of Experience (QoE) and Quality of Service (QoS), Privacy, Authentication and Node Localization.

3. Cryptography Algorithms

There are numerous cryptography algorithms available for various purposes. Some of those algorithms are directly used or adapted. Popular cryptography algorithms for WMSN include:

The symmetric encryption provides a single shared key for both encryption and decryption functions. As a result, the process of cryptography is easier to implement. However, the biggest challenge is how to securely distribute the shared key (AES, DES, IDEA). The standard symmetric encryption schemes, such as DES and AES, are commonly used. However, these schemes are unsuitable for multimedia data. Multimedia data is generally larger in size and use of these symmetric encryption schemes has memory and computation requirements not suitable for the sensor nodes, because its real time nature requires faster encryption.

The asymmetric encryption uses a pair of key stoppers to perform data encryption. A public key that is known by all nodes of the network is used to encrypt data, and a private key known only by the destination node is used to decrypt that data (RSA, ECC). Authors in many papers noted that asymmetric cryptography is not appropriate for WSN, because of its needs for more resource power and more processing time. Other papers have proven inversely. In the key based security management, if the decryption key is lost or corrupted during transmission, it is difficult to recover the information [13]. WMSNs asymmetric cryptography will be used more than symmetric cryptography because it makes a lot easier to solve several security problems related to eavesdropping and compromised nodes [3].

4. Multimedia Streaming and encryption

Streaming media is video or audio content sent in compressed form over the network and displayed immediately, rather than being saved to the secondary memories. Unlike scalar sensor networks, multimedia data include snapshots or streaming multimedia content. Snapshot multimedia data contains pictures obtained in a short period of time (still images). Streaming multimedia content is obtained over longer time periods and needs to be delivered in real time [2]. Video streaming supports military operations by delivering critical information rapidly and dependably to the right individual or organization at the right time. This improves the efficiency of combat operations. The new technologies must be integrated quickly to meet the requirements of present time. The same is for traffic monitoring [1]. In [14] the authors present problems in multimedia streaming where they elaborate that major problems when WMSN is used in surveillance are the lack of storage to save and record data, and the lack of services and battery consumption. Because of the lack of services the problems occur in the transfer of data, like data loss, quality degrade and low transfer rates. The authors also present some solutions to the aforementioned problems, and emphasize that the biggest problem is how to secure the data during transmission.

4.1. Multimedia Encryption Techniques

Multimedia sensors can sense and transmit data in the form of image, video and audio. As more data has to be encrypted and decrypted, cryptography naturally becomes more complex and resource-demanding in WMSNs. Because of the complex compression operations, the distributed environment and the limited bandwidth and power resources of WMSNs, there are inevitable needs for aggregation algorithms capable to decrease the total amount of information to transmit [15]. Images, video and audio have different particularities, and naturally, the cryptography mechanisms are different. In general, secure data transmissions can be achieved through symmetric or asymmetric cryptography, which may be performed through different algorithms. Both of those cryptography algorithms have pros and cons. Moreover, in the following text, multimedia cryptography techniques are presented, for each media type separately, as well as the most commonly used techniques.

4.2. Image Cryptography Techniques

Image sensors generate large amount of data traffic in a WMSNs, which may load the network bandwidth. The image data transmissions in WSNs can significantly degrade the network performance and sensor lifetime. The concept of secret sharing is used to develop a secure routing protocol. It works by dividing data packets (image) into smaller packets called shares, and these shares are sent through disjoint multipaths. An unauthorized user has to intercept at least a threshold number of those shares before the packet can be decrypted. In such case, unauthorized users must compromise all paths in order to decrypt the message. However, the drawback of this scheme is that the disjoint paths have to be determined before the shares are transmitted [5, 20]. Sending shares over already determined paths may not guarantee a video quality. In [16] authors are presenting data fusion techniques with algorithm of compressive sensing and watermarking, grouped in three data fusion categories: low-level fusion, medium-level fusion and high-level fusion.

4.3. Video Cryptography Techniques

Key challenges for video coding in the sensor nodes are also the low power and computational capabilities. For this reason, video sensors typically employ compression techniques based on coding mechanisms [7]. The videos are demanding more requirements of processing, memory, energy consumption, transmission delay and jitter, and more bandwidth than image transmissions. Their quality will depend on the resolution, the frame rate, the color pattern and the similarity between the reconstructed and original (source) video. These variables add complexity to the cryptography. An encryption algorithm for video streaming need to have at least two characteristics: the encryption time should be low to avoid delays and the compression rate of the video should not be decreased [21].

The idea of joint coding is to integrate encryption into compression operation by parameterization of the compression blocks, without modifying the compressed bits. Two main compression blocks, where these techniques have been applied, are Wavelet Transform and Entropy Coding. Advantages of JVCE is that, it compresses and encrypts information in a single operation, making it feasible for mobile and embedded devices to ensure multimedia security with their low power consumption. Considering this fact, JVCE reduce the latency of encryption operation which is useful for real-time video delivery. The fastest algorithm, like AES, is computationally very intensive for many of the real-time multimedia data.

Video scrambling method uses filter banks or frequency converters, and it is performing permutation of the signal in time domain or distortion of the signal in the frequency domain. This algorithm offers less security, and this method can be easily compromised. Other video coding algorithms may also be used for optimized cryptography [22]. The Distributed Video Coding (DVC) uses a video compression technique with low encoder complexity. The encoder can be very simple, but the decoder is significantly more complex [23].

Security and video quality are progressively significant attributes for wireless multimedia sensor networks. However, it is crucial to integrate security and video quality together for video transmission as delivering video data across a secure path does not often meet the video quality requirements in many traditional approaches.

4.4. Audio Cryptography Techniques

The way of how cryptography is performed depends on audio compression requirements, and in general, audio data compression requires less processing compared to the compression of images and video streams.

Pulse code modulation (PCM) is a technique that can be quite effectively encrypted, as both encryption and decryption are much simpler to execute. In this method, the audio signal samples will be encrypted using very common arithmetic algorithms and the total number of bits will be kept unaffected. The bandwidth required to transmit the encrypted signal is same as for the original signal. In the receiver section, the encrypted signal is decrypted using exactly the reverse algorithm used earlier for encryption [24].

CVSD is a type of delta modulation in which the step size of the approximated signal is progressively increased or decreased, as required, to make the approximated signal close match with the input analog wave.

Modified Discrete Cosine Transform (MDCT) is designed to be performed on consecutive blocks of a larger dataset, where subsequent blocks are overlapped so that the last half of one block coincides with the first half of the next block. This overlapping, in addition to the energy-compaction qualities of the DCT, makes the MDCT especially attractive for signal compression applications, since it helps to avoid artifacts stemming from the block boundaries [6, 25]. MDCT is employed in most modern lossy audio formats, including MP3, AC-3, Windows Media Audio, AAC. Similarly as with images and videos, audio streaming in wireless sensor networks can also be protected with watermarking.

4.5. Common cryptography techniques for all media types

Encrypting large size multimedia data might suffer high computation complexity and latency. The secret information cannot be recovered if the decryption key is lost or the encrypted content is corrupted during transmission [13].

The encryption of multimedia data may be very costly in time and computing power, which may be infeasible for some sensor networks [16]. To avoid this constrains, using selective encryption is the most appropriate way. In selective encryption, the basic idea is to encode only a set of blocks of sensed images. There are two coding algorithms which are well suited for selective encryption: quad-tree coding and wavelet coding [18]. Quad-tree coding is based on a computational rooted tree [4], which separate the original image into different sub-quadrants, which means that every node has zero or four sub-quadrants and reconstruction process is related to their position in the tree. While at DWT-based (Discrete Wavelet Transform) algorithms creates a hierarchy of frequency bands. DWT decomposes images into smaller parts, called sub-bands, each sub-band have different importance in original image reconstruction process [19]. Selective encryption technique is combining compression with encryption. This technique can handle real time audio and video data efficiently. This method selects only the most important coefficients of a compression process and encrypts those coefficients. Coefficients which are less important are not encrypted [17, 22]. To optimize the cryptography of video streams in wireless sensor networks selective encryption is used as well.

Another security mechanism used in protecting multimedia data is watermarking which provides authentication. Watermarking process hides authentication information in the original data. A digital watermark is a special marker that is embedded into scalar, audio, image or video data, aiming to provide a mechanism to identify ownership and copyright. The objective of digital watermarking is to protect the intellectual property of multimedia contents such as copyright protection, contents archiving, metadata insertion, broadcast monitoring, tamper detection and digital fingerprinting [15]. Watermarking system has two components: embedder (3 inputs: cover data, watermark, and key) and detector (1 input: key). In general, any media transmission over wireless sensor networks may be protected using watermarks. Also, watermarking is used in combination with others security mechanisms. However, watermarking solutions might be vulnerable to attacks from entities that know how the watermarks are done [3].

5. Conclusion

In this paper, we have surveyed the security threats and defending mechanisms in Wireless Multimedia Sensor Networks. WMSNs have been deployed in military sensing, traffic surveillance, target tracking, monitoring, and healthcare. We argue that DoS attacks are challenging problem in WMSN security. In this context, cryptography will play a central role in WMSN. There is symmetric and asymmetric encryption, and there are different advantages and drawbacks between them. Asymmetric cryptography will be used more than symmetric cryptography because it makes a lot easier to solve several security problems related to eavesdropping and compromised nodes. Images, videos and audios have different particularities, and cryptography is different for each media. The common encryption techniques like selective cryptography and watermarking have advantageous, but serious drawbacks for implementation in WMSNs exist. Considering the analyses conducted and the literature review, selective cryptography technique appears as the most appropriate approach suitable for securing data in WMSNs.

6. References

1. Vivek Katiyar, Narottam Chand, Naveen Chauhan;Recent advances and future trends in Wireless Sensor Networks,INTERNATIONAL JOURNAL OF APPLIED ENGINEERING RESEARCH, DINDIGUL Volume 1, Number (2010)
2. Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury; Wireless Multimedia Sensor Networks: Applications and Testbeds, Proceedings of the IEEE (2008)
3. Almalkawi, I.; Zapata, M.; Al-Karaki, J.; Morillo-Pozo, J. Wireless multimedia sensor networks: Current trends and future directions. Sensors (2010)
4. De Oliveira Gonçalves, D.; Costa, D.G. A Survey of Image Security in Wireless Sensor Networks. J. Imaging (2015)
5. Harjito, B.; Han, S. Wireless Multimedia Sensor Networks Applications and Security Challenges. In Proceedings of the International Conference on Broadband, Wireless Computing, Communication and Applications, Fukuoka, Japan (2010)
6. Daniel G. Costa *, Solenir Figuerêdo and Gledson Oliveira; Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions; MDPI (2017)
7. Satyajayant Misra, Martin Reisslein, and Guoliang Xue; A Survey of Multimedia Streaming in Wireless Sensor Networks, IEEE Communications Surveya & Tutorials, Volume 10, Number 4 (2008)
8. Luigi Alfredo Grieco, Gennaro Boggia, Sabrina Sicari, Pietro Colombo; Secure WMSN, Third International Conference on Mobile Ubiquitous Computing Systems, Services and Technologies (2009)
9. Wang, Y.; Attebury, G.; Ramamurthy, B. Security issues in wireless sensor networks: A survey. Int. J. Future Gener. Commun. Netw (2013)
10. Guerrero-Zapata·Ruken Zilan· José M. Barceló-Ordinas·Kemal Bicakci·Bulent Tavli; The future of security in Wireless Multimedia Sensor Networks; Published online: 3 December 2009 © Springer Science+Business Media (2009)
11. Sen, J. A Survey on Wireless Sensor Network Security. International Journal on Commun. Netw. Inf. Secur. (2009)
12. Modares, H.; Salleh, R.; Moravejosharieh, A. Overview of security issues in wireless sensor networks. In Proceedings of the International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, Malaysia, (2011)
13. Akshaya Gayathri, Ms. Suganthi, Saranya; Energy Efficient Image Transmission with Security in Wireless Sensor Networks, International Journal of Computer Applications in Engineering Sciences, Vol 3, Number 1(2013)
14. Himanshu Diwan, Pooja Agrawal, A.K.Dwivedi, Current Status and Design Challenges in Wireless Multimedia Sensor Networks, International Journal of Engineering Trends and Technology (IJETT) – Volume 6, Number 2 (2013)
15. Bambang Harjito, Elizabeth Chang; Secure communication in WMSN using watermarking; IEEE International Conference on Digital Ecosystems and Technologies (DEST), (2010)

16. Rui Gao, Yingyou Wen, Hong Zao; Secure Data Fusion in WMSN via Compressed Sensing, Journal of Sensors (2015)
17. Viral Patel, Krunal Panchal; Survey on Security in Multimedia Traffic in Wireless Sensor Network; IJEDR Volume 2, Issue 4, ISSN: 2321-9939 (2014)
18. Bhimrao S Patil Dept of CSE BKIT, Bhalki, Karnataka, INDIA; Image Security in Wireless Sensor Networks using wavelet coding; International Journal on Emerging Technologies - Special Issue on NCRIET (2015)
19. Costa,D.G.; Guedes,L.A. A discrete wavelet transform (DWT)- based energy-efficient selective retransmission mechanism for wireless image sensor networks. J.Sens Actuator Netw. (2012)
20. Rashwan, Honggang Wang, Dalei Wu, Xinming Huang; Security–quality aware routing for wireless multimedia sensor networks using secret sharing, SECURITY AND COMMUNICATION NETWORKS, (2015)
21. Varalakshmi, L.M.; Sudha, G.F.; Jaikishan, G. A selective encryption and energy efficient clustering scheme for video streaming in wireless sensor networks. Telecommun. Syst. (2014).
22. Pande A, Zambreno J. Embedded Multimedia Security Systems Algorithms and Architectures, (2013)
23. Bernd Girod (Fellow IEEE), Anne Margot Aaron, Shantanu Rane and David Rebollo-Monedero; Disturbed Video Coding, Proceedings of the IEEE 93 (2005)
24. Avijit Hira, Nazmus Sakib, Nayan Sarker; PCM based audio signal security system; International Conference on Advances in Electrical Engineering (ICAEE), (2013)
25. Honggang Wang, Michael Hempel, Dongming Peng, Wei Wang, Hamid Sharif, Hsiao-Hwa Chen; Index Based Selective Encrypton for WMSN; IEEE Transactions on Multimedia April (2010)