Secure Multimedia Transmission in wireless sensor network

Viral K Patel[1], Krunal J Panchal[2]
[1]*Student, L.J.Institute of Engineering and Technology*
[2]*Asst.Proff, L.J.Institute of Engineering and Technology*

***Abstract*- Wireless Multimedia Sensor Networks (WMSNs) are used in many application domains, such as surveillance systems, traffic control, process control and so on. In order to ensure a broad and effective 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 availability of resources in term of energy, computation, bandwidth, and storage on the 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. Because of the unprotected nature of wireless communication channel and untrusted transmission medium of wireless sensor networks, it becomes vulnerable to many types of security attacks. Also real-time multimedia streaming poses different challenges due complex nature of the information and the timeliness requirements. Also existing security approaches are difficult to implement on WSN due limited availability of the resources. The proposed algorithm will be implemented at application layer so that the packets containing encrypted data can be transmitted seamlessly.**

Index Terms- Wireless Multimedia Sensor Networks, Quality of Service, Security Simulator.

I. INTRODUCTION

Due to the recent development in computer networking, distribution of digital multimedia data over the internet is increasing. However, the multimedia processing tools, the increased number of digital documents and the availability of

Internet has created a very suitable medium for copyright fraud and uncontrollable distribution of multimedia data.[1.2]

In Wireless Communication Networks, wireless sensor networks (WSN) have gained significant importance in the last few years. Currently WSNs are targeting a number of applications ranging from military and civil application to modern healthcare. WSN are basically comprised of scalar sensors which are capable of collecting information from physical environment, processing it and transmitting the processed information to remote server or centralized system.

Now, the availability of complementary metal-oxide semiconductor (CMOS) camera and small microphones make possible the development of Wireless Multimedia Sensor Network (WMSN), i.e. networks of wirelessly interconnected devices that allow retrieving video and audio streams, still images, and scalar sensor data.[3]

As wireless sensor networks continue to grow, there is a need for effective security mechanism. Because sensor networks may be interace with sensitive data and operate in hostile unattended environment, it is important that the security concerns be addressed from the beginning of system design. Due to inherent resource and computing constraints, security in wireless multimedia sensor networks poses different challenges than traditional network/computer security. Earlier research targets the challenges by WSNs like limited node computational and communication power, power resources and scalability etc. Now with the recent development of WMSNs additional challenges are added which must also need to be addressed i.e. application specific QOS (Quality of Service) constraints, coverage area of sensor nodes, high bandwidth demand because of the large size multimedia data and the most important is the security mechanism to prevent this multimedia content.[4,5]

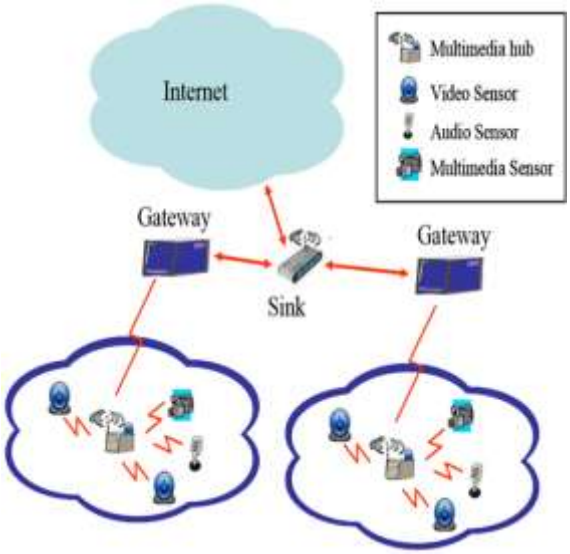


Figure 1.1: Wireless Multimedia Sensor Networks Architecture

A wireless multimedia sensor network is an emerging field of research and the security of the multimedia data is one of the major issue. Here we are dealing with the multimedia data such as video, audio and images so it is also important to focus on the efficient security algorithm to prevent our multimedia data. Another issue is, after applying so many security techniques, the performance of the network and data retrieval process should not be affected.

The high and ever growing availability of low cost multimedia devices (such as video camera and microphones with CMOS technology) and wireless communication systems (such as those proposed by the families of standards IEEE 802.11 and 802.15) fostered the development of Wireless Multimedia Sensor Networks (WMSNs). The CMOS technology allows one to embed into 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 . Such an input device can be connected (by means of modules Cyclops) to already available wireless sensors (for instance Crossbow, MICA2 or MICAZ). The resulting connection is a multimedia sensor equipped with images acquisition and processing functionalities, communication interfaces, memory modules, power supply and control units. Imote, Imote2 and Stargate are some other examples of recently released multimedia sensors. A WMSN is composed of numerous multimedia sensors that exchange sensed data with sinks using a wireless channel. The need 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 [810,14], the computational complexity of compression, aggregation, and distributed processing, the overload to manage security/privacy policies and Quality of Service (QoS). During the last few years, Wireless Multimedia Sensor Networks (WMSNs) appeared. WMSNs technology have emerged due to the production of cheap CMOS (Complementary Metal Oxide Semiconductor) cameras and microphones, which can catch rich media content from the environment like images and videos. WMSN can be defined as networks of wirelessly interconnected sensor nodes equipped with multimedia devices, such as cameras that are capable of retrieving video and audio streams, images, and scalar sensor data. WMSNs are currently being used in several applications as outlined below.[1]

A. Multimedia surveillance sensor networks

Multimedia surveillance applications are used to detect, recognize and track the objects in order to take appropriate actions. These applications need to continuously capture images in order to monitor certain events. These applications are mainly used for detecting crimes or terrorist attacks.

B. Traffic avoidance and control systems

Traffic avoidance applications are used to monitor car traffic and provide traffic routing advice to avoid congestion. M. Jokela proposed a model of three different kinds of cameras to be used in monitoring a traffic situation around a vehicle to detect problems such as a near infrared camera, a thermal imaging system for animal detection, and a regular CCTV camera for ice and snow detection.

C. Advanced health care delivery

Health and care delivery applications are used for patient monitoring and care in remote sites like monitoring patients' facial expression, respiratory conditions or movement and forward these images to doctors in distant hospitals to make better diagnosis. In a healthcare sensor periodically captures vital

signs information (e.g., body temperature, Blood pressure) and sends it to the gateway. Once the information processed by the gateway, it is forwarded to doctors to help them make an initial diagnosis. After that, wireless multimedia sensor nodes used to capture and send back images or videos data to help doctors obtain more detailed information and make final diagnosis.

D. Automated parking advice

Automated parking advice applications keep track of available parking spaces and provide guidance to the drivers to allocate free parking spaces.

E. Environmental monitoring

Environmental monitoring application used for monitoring remote and unreachable areas over a long period of time. In these applications, energy-efficient operation are particularly important in order to extend monitoring over a long period of time. Most of the time cameras are combined with other types of sensors into a heterogeneous network, so that cameras are triggered only when an event is detected by other lighter sensors used in the network.

II.AUTHENTICATION AND SECURE LOCALIZATION

So far only a part of the security solutions used in WMSNs fully complies with the peculiarities of these networks. In some cases, known methods 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.Issues of authentication and secure localization information fall in the general problem of the trust management. In a distributed an environment like a WMSN, trust management becomes a 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 requirement. Sensor 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. 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, few solutions are available, 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. STANDARD TECHNIQUES

Information security has traditionally been ensured with Encryption techniques. Generally encryption techniques, such as the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), the Rivest, Shamir and Adelman (RSA) algorithm, the Triple DES (3DES), and the International Data Encryption Algorithm (IDEA) and Scalable encryption algorithm(SEA), work on bit stream of data input without regard to their nature of application. In other Words, the encryption proceeds without distinguishing the input data as either: audio, text, video.

ENCRYPTION ALGORITHM	BASIC OPERATION	ADVANTAGES AND DRAWBACKS
DES	XOR, Substitution and Permutation	Suitable for High speed and low cost hardware/software implementations. But Small 56 bit key size makes it undesirable.
3-DES	Comprises 3 DES keys	Efficient and susceptible to chosen plaintext, but memory and time requirement is more
AES	Sub bytes, Shift rows, Mix column and add round key	Very good performance in hardware and software implementations, Low

		Memory requirement
IDEA	XOR, Addition and Multiplication	Security level is high when compared to DES.
RSA	Primality test, Modulus, Euler's totient Function, Co prime and Multiplicative inverse	It is Public key system. Secured but speed is lower, when compared to Symmetric key systems.
SEA	XOR,S-Box, Word rotation, bit Rotation and modular addition	Extremely simple but can be used only in embedded applications where resources are limited.

Table 3.1

When the Multimedia data is not a real time data, it can be treated as a regular binary stream and above mentioned conventional techniques can be applied. When varieties of constraints are present, it is difficult to accomplish security for multimedia data.

A. Video Encryption

Symmetric key cryptography algorithms can be used to encrypt the multimedia data. But the fastest algorithm, such as AES, is computationally very costly for many of the real-time multimedia data.

1) Video scrambling

This 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. However, this scheme is offering less security, and this method can be easily cracked by advanced computers [2].

2) Selective Video encryption

Selective encryption technique is combining compression with encryption. This technique can handle real time audio and video data efficiently. This method is selecting only the very important coefficients from final or intermediate steps of a compression process and encrypt those coefficients. Coefficients which are less important not encrypted.

a) Secure MPEG (SECMPEG)

The SECMPEG contains four different levels of security. At the very first phase, SECMPEG encrypt the headers from the sequence layer to the slice layer, while the motion vector and DCT block are unencrypted. At the second phase, most relevant part of the I-blocks are additionally encrypted (upper left corner of the block). At the third level, SECMPEG encrypts all I-frames and all I-blocks. At the fourth level, SECMPEG encrypt the whole MPEG-1 sequence (the naive approach).

b) Aegis

Aegis was initially designed for MPEG-1 and MPEG-2 video standards. Aegis method encrypts I-frames of all MPEG groups of frames in an MPEG video stream, while B- and P frames are unencrypted. In addition, Aegis encrypt the MPEG video sequence header, contains all of the decoding initialization parameters which include the picture width, bit rate, height, frame rate, buffer size, etc. This method provides sufficient security for the entertainment videos, such as the pay TV broadcast, but not satisfying the applications where the security is one of the top priorities.

c) Zigzag Permutation Algorithm

This algorithm is based on embedding the encryption into the MPEG compression process. JPEG images and the I-frames of MPEG video undergo a zigzag reordering of the 8x8 blocks. The zigzag pattern makes a sequence of 64 entries that is ready to enter entropy-encoding stage. The main purpose of this approach is to use a random permutation list to map the individual 8x8 blocks to a 1x64 vector. Zig zag permutation cipher seriously lacks the desired level of security.

d) Shi - Wang - Bhargava Video Encryption Algorithms

Shi, Wang and Bhargava have classified their work into four different Video encryption algorithms.

d.1) Algorithm I

This algorithm uses the permutation of Huffman code words in the I-frames. And incorporates encryption and compression in one step. The secret part of the algorithm is a permutation p, which is used to permute standard JPEG/MPEG Huffman code word list. To save compression ratio, the permutation p should be such that it only permutes the code words with the same number of bits. But this algorithm is highly vulnerable to known-plaintext attack, and cipher text-only attack.

d.2) Algorithm II (VEA)

This algorithm encrypts only the sign bits of the DCT coefficients in an MPEG video. The Algorithm II simply xors the sign bits of the DCT coefficients with a secret m-bit binary key k = k1k2…km. The security of this algorithm depends on length of the key. If the key is as long as the video stream and it is unique and used only once which is known to be absolutely secure. But this is highly impractical for mass applications such as VOD (Video on Demand) and similar. On the other hand, if the key is too short, many attacks can be developed.

B. Audio and Speech Encryption Techniques

Secure voice (alternatively secure speech or ciphony) is a term in cryptography for the encryption of voice communication over a range of communication types such as radio, telephone or IP. It is enough to apply the naïve approach, but in many instances this is too computationally expensive in the case of small mobile devices. As far as the security is concerned, perhaps the most important type of audio data is speech. Unlike in the case of music files and similar entertainment audio sequences, in many applications, speech requires substantial level of security.

1) Encryption of compressed speech

Speech signals are encrypted simply by permutation of speech segments in the time domain or distort the signal in the frequency domain by applying inverters and filter banks. But this method is insecure.

2) B. Encryption of compressed Audio

There are numerous applications where the general audio data needs to be protected, and the expensive naive approach might be infeasible. In the case of MP3 (MPEGI, Layer3), selective encryption is implemented in which the MDCT (Modified cosine transform) coefficients are partitioned into several frequency regions during Huffman encoding. This spectral subdivision may be exploited to lower the perceptual quality of the compressed signal by low-pass filtering.

C. Image Encryption Techniques

Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. However, there are number of applications for which the naive based encryption and decryption represents a major bottleneck in communication and processing. So in that cases selective image encryption techniques are used. Selective image encryption is based on encrypting only certain parts of the image, in order to reduce the amount of computation.

1) Partial Encryption Schemes

Partial encryption methods that are suitable for images, compressed with two classes of compression algorithms. They are quadtree compression algorithms, and wavelet compression algorithms based on zero trees. Partial encryption scheme encrypts only the significance information related to pixels.

2) Selective Encryption Methods

An uncompressed (raster) grey level image defines 8 bit planes. The highest (most significant) Bit planes are highly correlated to the original gray level image. This selective encryption scheme that is consisted of xoring the selected bit planes with a key that has the same number of bits as the bits that are to be encrypted. Encrypting only the bit planes that contain nearly uncorrelated values would decrease the vulnerability to the known-plaintext attacks. In this selective encryption method, only the appended bits that correspond to the selected AC coefficients are encrypted. The DC coefficients are left unencrypted, since their values are highly predictable. On the other hand, the code words are left unencrypted for the synchronization purposes.

IV. IMPLEMENTATION

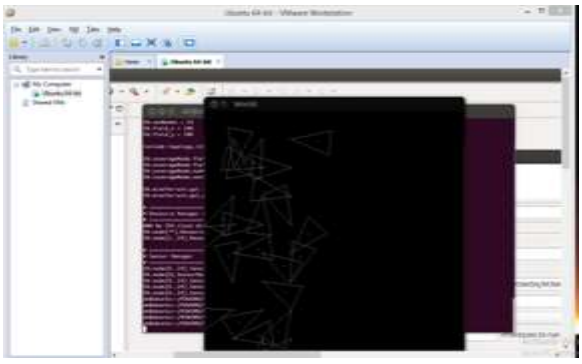


Figure – 4.1

In the figure 4.1, the nodes are catching the data. The YUV data is converted into mpeg file and then converted into mp4 file. Finally this mp4 file converted into text file. This text file is the input to the gpsr routing protocol where security mechanism is applied to it.

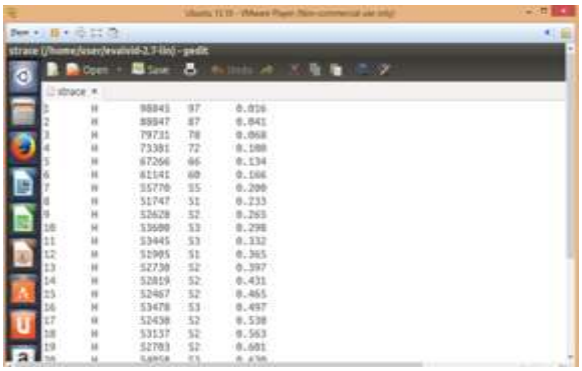


Figure 4.2

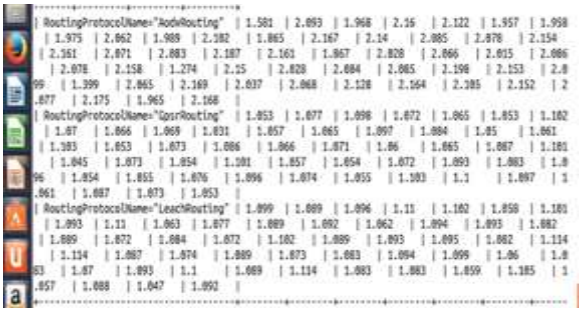


Figure 4.3

In the above figure, the patching and performance of routing protocols AODV, Leach and GPSR is showed. Figure 4.6 shows that the consumed energy by gpsr routing protocol is less. Figure 4.7 shows the node wise energy of 50 nodes for the same three protocols and figure 4.8 shows the average energy consumed by each routing protocol. So by all these three result, it is better to use gpsr routing protocol for the implementation.

After the AES encryption and CMAC code generation, there are two files generated which are given below. These two files will be used to regenerate the original video file.

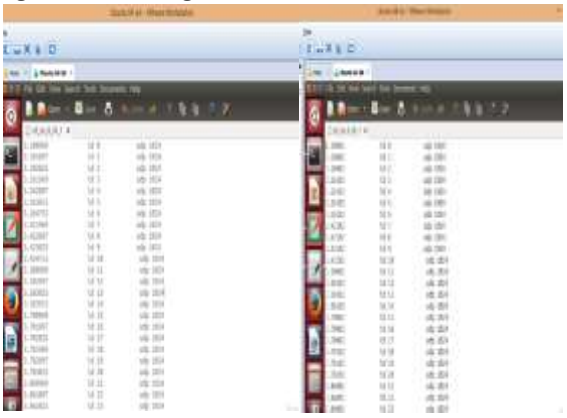
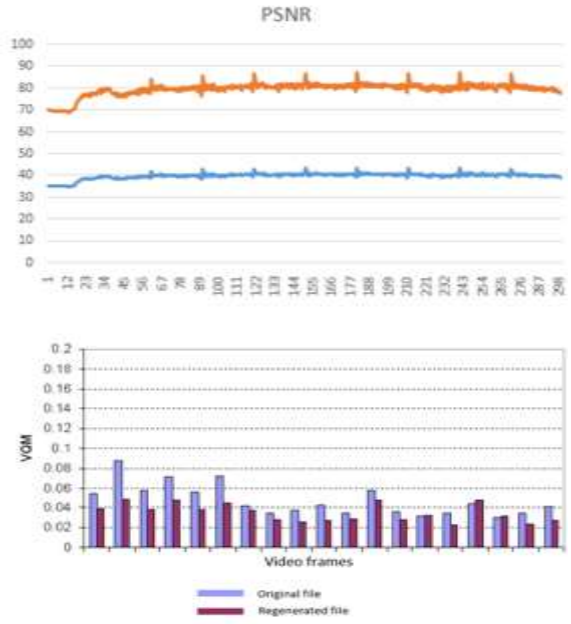


Figure 4.4

These generated files will be converted to video file called regenerated_video.mp4 and we can compare the original file hall_h264_128 with this regenerated_video.mp4 file. The PSNR graph is generated and the PSNR ratio in the figure 4.10 indicate that the the regenerated file is is very much close to the original file in terms of clearity and complexity and the distortion and noise is very less after applying all security features.



V. CONCLUSION

This paper has presented a literature review of the different security technology of multimedia data in wireless multimedia sensor network. It is easily understandable that the existing security methods have some drawbacks. Some advanced methods are quite difficult to implement in real time. It is necessary to protect the multimedia data and there is a need of special technique to protect this type of data which provide confidentiality, authentication and integrity.

REFERENCES

[1] Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury, "A Survey On Wireless Multimedia Sensor Networks", Computer Networks (ELSEVIER), Vol 51, Pages 921-960, 2007.

[2] K.Kalaivani, B.R. Sivakumar, "Surey On Multimedia Data Security", International Jounal Of Modeling and Optimization, Vol 2, February 2012.

[3] Atif Sharif, Vidyasagar Potdar, Elizabeth Chang, "Wireless Multimedia Sensor Network Technology: A Survey", 7th IEEE international conference on IEEE, 2009.

[4] John Paul, Zhengqiang Liang, "Wireless Sensor Network Security: A Survey", Security In Distributed, Grid And Pervasive Computing, CRC Press, 2006.

[5] Luigi Alfredo Grieco, Gennaro Boggia, "Secure Wireless Multimedia Sensor Networks: A Survey", 3rd international conference on Mobile Uboquitous Computing, Sysems, Services and Technologies, IEEE 2009.

[6] Jyotsna Suryadevara, Bollam Sunil, Nagender Kumar, "Secured Multimedia Authentication System For Wireless Sensor Network Data Related to Internet Of Things", 7th international conference on Sensing Technology, Pages 109-115, IEEE 2013.

[7] Nour El Deen M.Khalifa, Mohamed Hamed N. Taha, Hesham N. Elmahdy, Imane Saroit, "A Secure Energy Efficient Schema for Wireless Multimedia Sensor Networks", International Journal of Wireless Communication, Vol 5, No 6, June 2013.

[8] M.RAVI, G.V ITHYA, "Qos with Security in Wireless Multimedia Sensor Networks", International Journal of Computer Networks and Wireless Communication", Vol.2, No.3, June 2012.

[9] Ersin Elbaşı, Suat Özdemir, "Secure Data Aggregation in Wireless Multimedia Sensor Networks via Watermarking", Application of Information And Communication Technologies, IEEE 2012.

[10] Amit Pande, Prasant Mohapatra, "Securing Multimedia Content Using Joint Compression and Encryption", Multimedia, Volume 20, Issue 4, IEEE 2013.