EDES- Efficient dynamic selective encryption framework to secure multimedia traffic in wireless sensor networks

Abderrezak Rachedi, Kaddar Lamia, Ahmed Mehaoua

EDES- Efficient Dynamic Selective Encryption Framework to Secure Multimedia Traffic in Wireless Sensor Networks

Abderrezak Rachedi*, Lamia Kaddar†, and Ahmed Mehaoua‡§
*University of Paris-Est, Computer Science Laboratory (LIGM UMR 8049),
Champs-sur-Marne, France. Email: rachedi@univ-mlv.fr
†University of Versailles, PRiSM Lab., Versailles, France
Email: lamia.kaddar@prism.uvsq.fr
‡LIPADE Laboratory, University Paris Descartes,Paris, France
Email:ahmed.mehaoua@mi.parisdescartes.fr
§Division of IT Convergence Engineering, POSTECH, Korea

***Abstract*—In this paper we propose a new framework able to ensure security, multimedia quality and energy efficiency in Multimedia Wireless Sensor Networks (MWSNs). The energy is an important and limited resource, which has a direct impact on the lifetime of nodes in MWSNs. In addition, the characteristics of MWSNs like the limited bandwidth and non-deterministic channel access have a significant impact on the QoS of multimedia traffic. We propose the Efficient Dynamic Selective Encryption Framework (EDES) in order to reduce the energy consumption and increase the QoS while ensuring a secure multimedia traffic. EDES proposes three security levels (high, medium and low) and the selection of each level depends on the energy and QoS parameters. Moreover, the cross-layer approach is selected for EDES to take into account the different parameters at physical, MAC and upper layers. The capacity metric is proposed to evaluate the possibility to increase or decrease the security level. The simulation results illustrate the importance of the security level adaptation according to the QoS and the energy parameters. EDES increases the lifetime duration of nodes by almost 40% compared to static encryption.**

I. Introduction

The Multimedia Wireless Sensor Networks (MWSNs) have gained the interest of researchers and industrials, because of their large applications. Unlike the Wireless Scalar Sensor Networks (WSSNs), MWSNs offer new network services like video and audio communications. The application fields of MWSN are mainly related to security such as: video surveillance, people or objects tracking, border monitoring, etc [1][2]. Therefore, these applications require security services like the end-to-end data confidentiality between the multimedia sensors and the server (sink), the mutual authentication, and the data integrity. However, the characteristics of MWSNs such as: the limited resources (bandwidth, energy, memory and processing), the wireless link and mobility make the proposition of an efficient security solution a real challenge. Many solutions proposed to secure both WSSNs and MWSNs are mainly based on static public or symmetric cryptography algorithms [3]. In the case of public cryptography the Elliptic Curve Cryptography (ECC) implemented in hardware [4] or software [5] is used. However, in the case of symmetric cryptography, the Tesla and micro Tesla [6] are used. Most security solutions proposed for MWSNs do not only encounter the energy constraint but also the QoS constraints. We know that the security cost can directly impact the network performance and QoS. For instance, when the size of packets increases because of the addition of security information like numerical packet signature, the data throughput of data decreases.

Unlike existing works, which focus on security, QoS and energy separately, we introduce in this work the security of the multimedia traffic while taking into account QoS and energy. We propose a new framework called EDES able to adapt the security levels according to QoS and energy parameters. The basic idea of EDES is to improve security in terms of robustness without negatively impacting the QoS and lifetime of sensors. We introduce a new metric called capacity to assess the available resources in terms of throughput, delay, link quality and energy. The cross-layer approach is selected to correctly evaluate the different parameters at different layers. Moreover, the different types of video frames do not have the same importance. The compression exploits temporal and spatial correlations in an image sequence, so there is a dependency between frames created by the inter-frame coding. Inter-frame coding uses motion estimation and compensation between successive video frames. For instance, in the case of MPEG4 codec the frame types P and B need the adjacent frame I and frame P respectively in order to be correctly decoded. In other words, it is not possible to rebuild frames P and B without the data in frames I and P respectively. Therefore, the frame types significance is not the same. That is why, we use in this work the selective encryption process to differentiate between different frames.

The rest of the paper is organized as follows: in section 2, we present the summarization of the existing works related

This research was funded by LIGM (CNRS UMR8049) and partially supported by the Korea Science and Engineering Foundation, under the WCU (World Class University) program.

to security and encryption in MWSNs. Section 3 presents our proposed solution Efficient Dynamic Selective Encryption Framework (EDES). The fourth section is dedicated to the results obtained with the simulators and their analysis. Finally, section 5 concludes the paper and presents our future works.

II. Related Works

Recent works dealing with Quality of Service (QoS) in MWSNs are mainly focused on the QoS maximization and energy consumption minimization. Kandris et al. [7] proposed a scheme called PEMuR which aims at saving energy and maximizing the QoS rate for an efficient video communication. PEMuR proposes the combined use of an energy aware hierarchical routing protocol with an intelligent video packet scheduling algorithm. This algorithm may cope with limited available channel bandwidth by selectively dropping less significant packets prior to their transmission. Another work proposed by Cobo et al. [8] dealt with the QoS routing model for Wireless Multimedia Sensor Networks (WMSN). The proposed solution called AntSensNet is based on the traditional ant-based algorithm and multi-QoS routing metric. However, these solutions did not deal with security issues.

Other proposed solutions dealt with security in the case of low-power computing and communication devices by using a selective encryption concept. The idea of selective encryption is to encrypt chosen units of message while leaving the remaining units unencrypted. This concept was introduced by Spanos and Maples in [9]. Meyer and Gadegast [10] propose to reduce the amount of encrypted MPEG data in a video sequence while at the same time providing an acceptable level of security. However, these works did not take into account the constraints of Multimedia Wireless Sensor Networks (MWSNs). In addition, main works on selective encryption focused on performance issues and not on security issues. That is why, Lundin and Lindskog have evaluated the security impact of the selective encryption by using the entropy and guesswork [11]. In this work, we combine between opposite QoS and security parameters with energy consumption consideration.

III. Efficient Dynamic Selective Encryption Framework

The Efficient Dynamic Selective Encryption framework (EDES) is based on two main steps. The first step consists in assessing the network performance parameters. We introduce the new capacity function called CAP. This function combines between QoS parameters and residual energy. The QoS parameters consist of the throughput, delay and link quality. In order to assess these parameters, we select the cross-layer approach which is able to deal with MAC, routing and other upper layers parameters. The second step consists in selecting a security level and using or not the selective encryption algorithm. The security level is selected according to the CAP function. The capacity function allows to evaluate the resources availability at the transmitter camera sensor node and it is based on four parameters: the throughput, the delay, the link quality index (LQI) and the residual energy. The throughput and the delay are the most important parameters for multimedia traffic. We know that this kind of traffic needs an important throughput and minimum delay. The strategy of CAP function is summarized as follows:

- Maximize the residual energy of the camera sensor (RE)
- Maximize the throughput
- Maximize the Link Quality Index (LQI)
- Minimize the delay

The CAP function between two nodes i and j can be expressed according to the chosen QoS metrics:

$$CAP_{i,j} = \sum_k c_k \times f_k(x_{ij}^k) \tag{1}$$

where x_{ij}^k is the value of metric k relatively to the link between two nodes i and j, c_k is the preference weight of metric k with $\sum_k c_k = 1$, and $f_k(:)$ is a normalized function. x_{ij}^k presents the following QoS parameters: Throughput, Delay, Link quality and Residual energy. The choice of the weights c_i depends on the application and the type of traffic (the delay is more important than the loss rate for streaming). CAP function introduces four formalized functions $f_k(:)$. The normalized function is introduced to express different characteristics of different units with a comparable numerical representation. The most commonly used normalized functions are the sigmoidal (S-shaped) functions. Indeed, sigmoidal functions are well-known functions often used to describe QoS perception [12]. We consider the following analytic expression for the sigmoid form:

$$f(x) = \frac{(x - x_m)^\zeta}{1 + (x - x_m)^\zeta} \tag{2}$$

where $x_m > 0$ and $\zeta \geq 2$ are tunable parameters, according to which different users' utilities are differentiated.

EDES defines three security levels: low, medium and high. The low security enables the receiver nodes to control the data integrity and the sender authentication by using the Hashed-based Message Authentication Code (HMAC). However, this level does not ensure the data confidentiality. The medium level has the same security services as low level and ensures data confidentiality by using Standard (AES) algorithm. If the network traffic requires confidentiality, EDES chooses whether the medium or the high security level according to the network status. In this work, we did not focus on the cryptographic keys distribution. In MWSNs the camera sensors send the data to the sink node (Many-to-one communication). We assume that the multimedia sensor nodes shared secret keys with the sink node and all known nodes shared the secret group key [13]. The difference between the high and medium security levels is the percentage of encryption which is higher than $\%Th_{high}$ in the case of a high security level. In addition, EDES differentiates between the frame types in order to select the important frame called key-frame (ie. frame I in the case of MPEG-4 codec). The percentage of encryption in the case of I frame is not the same for other frames. In this work, we consider two types of video codecs: MPEG4 and H263. In both codecs, I and PB frames are important frames in MPEG4

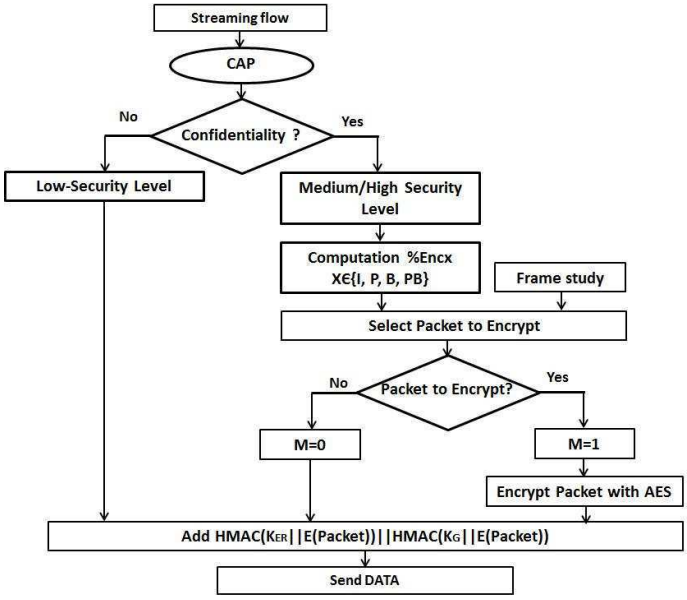

Fig. 1. Flowchart of EDES at the Sender node

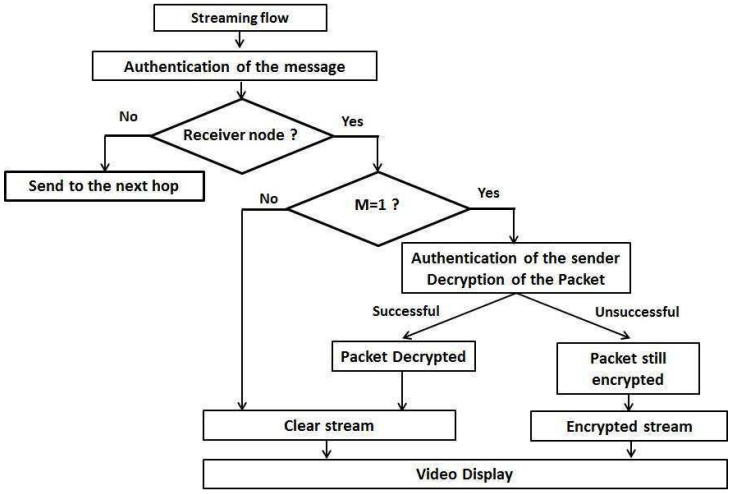

Fig. 2. Flowchart of EDES at the Receiver node

and H263 respectively and the percentage of their encryption is Enc_I. The encryption percentage of other frames depends on Enc_I and their computing is given as fellows:

In the case of MPEG 4 video coding:

$$\begin{cases} P-frame\_Encryption = Enc_P = C_P * Enc_I \\ B-frame\_Encryption = Enc_B = C_B * Enc_I \end{cases}$$

In case of h263 video coding:

$$\begin{cases} P-frame\_Encryption = Enc_P = Enc_I \\ PB-frame\_Encryption = Enc_{PB} = C_{PB} * Enc_P \end{cases}$$

Where C_P, C_B and C_{PB} are coefficients of importance of P, B and PB frames compared to I frames. In the case of H263 the frame P has the same importance as frame I (Enc_I = Enc_P). In order to switch between three security levels, we define three CAP thresholds values. The high security level needs a sufficient network performance and residual energy. The medium security level is an intermediate level which enables to ensure the confidentiality with an acceptable resource consumption. Without enough resource availability the minimum security is ensured by the low level. The following equation defines the switching between different security levels:

$$\begin{cases} if(CAP \geq \%Th_{high}) & Enc_I = \%Th_{high} \\ if(\%Th_{min} \leq CAP \leq \%Th_{high}) & Enc_I = 50\% \\ if(CAP \leq \%Th_{min}) & Enc_I = 0\% \end{cases}$$

where Th_{high} and Th_{min} can be tuned according to wireless nodes technologies and the desirable security.

EDES framework can be summarized into two flowcharts illustrated in figures 1 and 2. Figure 1 shows the set of operations executed by the sender. The CAP function assesses the resource availability in terms of network performance parameters and residual energy. If the network traffic needs confidentiality, the low security level is discarded. The specific operations are launched according to the selected security level. In the case of low security level the information related to data integrity and authentication is added by using two HMAC: first one is based on group key (K_G) for the relayed nodes and and the second one is based on the key shared by the sensor camera and the sink node (K_{ER}). The key group enables the relayed node to check if the packet is generated by authorized network member nodes and the data integrity. This HMAC is changed at each hop in order to check each relayed node. This is a common operation between the different security levels. However, in the case of high and medium security levels, the frame study and encryption percentage of each type of frame is specified. Moreover, information (M) is added to indicate if the packet is encrypted or not. The selective encryption is carried out according to the chosen $\%Enc_I$ of each frame. Finally the digital packet signature is added for authentication and data integrity.

Figure 2 shows the flowchart at the receiver node (sink or relayed node). When the relayed node receives the packet, it checks the HMAC associated with the packet. If it is correct, the packet is relayed or generated by an authenticated node using K_G. If the receiver is the sink node, it checks the HMAC by using the secret shared key (K_{ER}) before the decryption process. If the operation is succeeds the decryption process is applied.

IV. Performance Evaluation

In order to evaluate the performance of EDES, we simulate the proposed selective encryption algorithms and CAP function by using $NS2$ [14] and $Mica2dot$ characteristics platform [15]. We used two different video codecs: MPEG4 with low quality and H263 with $16kbps$ rate. The basic difference between both video codecs is that in MPEG4 coding all the important information are in the I-frame, for example the average of I-frames is 7000 bytes, whereas the average size of P-frames is 300 bytes and less than 100 bytes for B-frames.

TABLE I
NS2 SIMULATION PARAMETERS

MAC/Physical Technology	IEEE802.15.4
Packet size	127 Bytes
Th_{min}/Th_{high}	20 / 60
C_P / C_B / C_{PB}	0.5 / 0.5 / 0.5
Number of mobile nodes	25
Routing protocol	AODV
CBR/VBR rates	16kb/s
Maximum throughput	150Kbps
Simulation time	100s

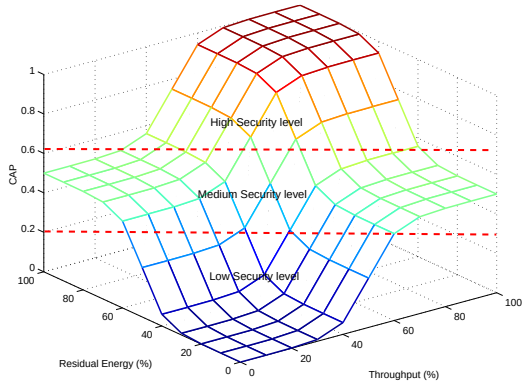

Fig. 3. CAP versus Residual energy

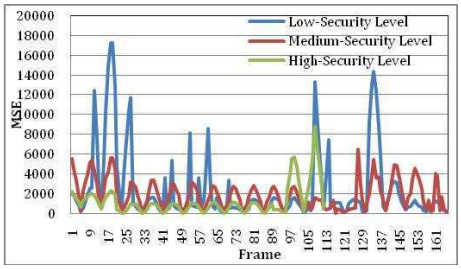

Fig. 4. MSE measure of the encrypted videos

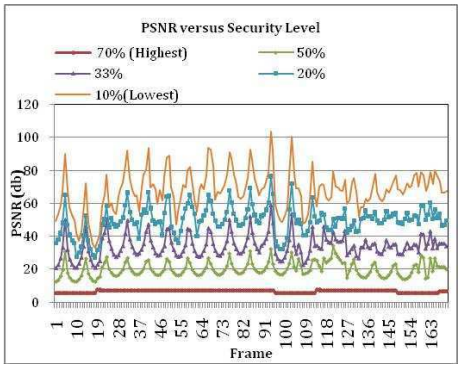

Fig. 5. PSNR versus Security Levels

However, with H263 there is only one I-frame (the first one) then the frame's size is distributed between PB-frames and B-frames and the PB-frames are more frequent than the I-frames in MPEG4. Moreover, the simulation parameters are presented in Table I.

A. CAP function performance

The obtained simulation results are plotted in Figure 3 which shows the CAP function behavior with different parameters such as: the residual energy, throughput and link quality. We remark that the high security level is reached when both parameters: throughput and residual energy are high otherwise the medium security level depends on the selected Th_{min}.

B. Evaluation of Security

In order to evaluate the security aspect, we used $SecVLC$ tool [16]. We select a video with a high rate of movement as testbed in order to evaluate the performance of EDES in terms of security, energy consumption and network lifetime. MSU Video Quality Measurement Tool (MSU VQMT) [17] is used to analyse the quality of different videos. This application enables to carry out an objective comparison of the different video codecs and to perform filters in the video analysis.

We used MSE (Mean Square Error) as metric to evaluate the image quality. MSE measures the average of "errors" squares. It assesses the quality of an estimator according to its variation. When MSE is low the loss of information for a potential attacker is high. Figure 4 shows MSE versus frames with different security levels. We remark that MSE increases significantly between two frames encrypted with a low-security and medium-security level. MSE is relatively stable with $Enc_I = 20\%$.

We used $PSNR$ (Peak Signal-to-Noise Ratio) [18] as another metric in order to evaluate the power of signal and power of corrupting the noise which affects the quality of video representation. Typical values for the $PSNR$ in lossy image and video compression are between 30 and 50 dB, where higher is better. Acceptable values for wireless transmission quality loss are considered to be about 20 dB to 25 dB.

Figure 5 shows the average PSNR versus frames with different security levels varying from highest $Enc_I = 70\%$ to lowest $Enc_I = 10\%$. We remark that the PSNR decreases when the percentage of I-frame encryption increases. In the case of $Enc_I = 70\%$ the PSNR is around $6.68db$ which is a very low value. However, when $Enc_I = 33\%$ and 10% the PSNR is $14.08dB$ and $17.99dB$ respectively which are high values. Despite the low encryption percentage, the PSNR does not exceed $18db$ which is lower than $20dB$ and $25dB$.

C. Energy Saving Evaluation

We know that the cost of energy consumption by the cryptography algorithms is inferior to the cost of radio communication [15]. The equations to compute the energy consumption in the case of transmission and reception are as follows:

$$\begin{cases} ETx = Packetsize * 59,2\mu Joule \\ ERx = Packetsize * 28,6\mu Joule \end{cases}$$

where $28,6\mu Joule$ is the cost of receiving one byte and $59,2\mu Joule$ is the required cost to transmit one byte.

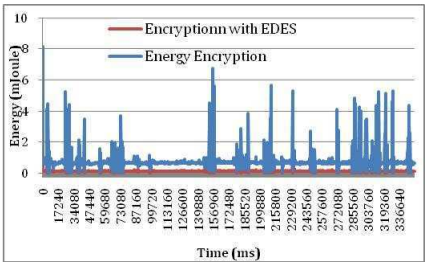

Fig. 6. Encryption Energy Consumption

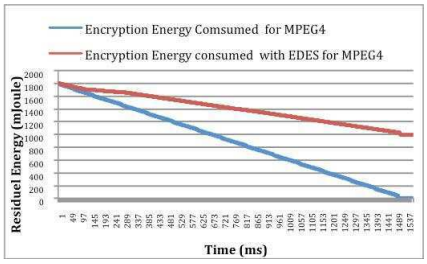

Fig. 7. Encryption Energy comsumption for MPEG4 low quality video

Let's consider the case of a sensor node using $2 \times AA$ batteries. That means that the initial battery of a sensor is $2 \times 2700mAh$. We know that $1wh = 3600joule$, then the initial energy expressed in joule is $E_{Initial} = 17820Joule$.

Figure 6 illustrates the encryption energy consumption versus time with EDES and the classical encryption algorithm. We remark that the energy consumption of EDES is significantly inferior to and more stable than the classical encryption algorithm. The high variation of energy consumption in the case of the classical algorithm is mainly due to the encryption of all frames because the frames size variation directly impacts the energy consumption and it is not the case with EDES.

In order to evaluate EDES with both video codecs: MPEG4 and H263, we simulate EDES and the obtained results are plotted in figure 7. We remark that using H263 video codec with EDES increases the MWSN lifetime by around 50% compared to MPEG4. We conclude that H263 is more adapted to MWSNs characteristics. Moreover, EDES improves the lifetime by 40% compared to the classical encryption algorithm. The reduction of energy consumption is more important at the source node compared to the destination node, because in MWSNs the destination node is the sink node (server). Therefore, the impact at the receiver node can be neglected in MWSNs.

V. Conclusion

In this paper, we proposed a new framework called Efficient Dynamic Selective Encryption Framework (EDES) in order to ensure dynamic security levels while taking into account the network performance and the energy consumption. The innovation of the proposed EDES consists in the combination of QoS parameters and security levels. EDES proposes three security levels (high, medium and low) with the ability to ensure the authentication, the data integrity and the confidentiality. The selection of each level depends on the energy and QoS parameters. The capacity function is proposed to evaluate the possibility to increase or decrease the security level. The assessment of this function is based on the cross-layer approach to take into account the different parameters at physical, MAC and upper layers. The simulation results illustrate that the security is ensured even with a low security level. In addition, EDES increases the lifetime duration of nodes by around 40% compared to the classical encryption algorithm. In our future works, we plan to extend our study to dynamic MWSNs by taking into account a new parameter: mobility.

References

[1] Ian F. Akyildiz, T. Melodia and Kaushik R. Chowdhury, *A survey on wireless multimedia sensor networks*, Journal of Computer Networks, Volume 51, Issue 4, 2007

[2] I. Boulanouar, A. Rachedi, S. Lohier, G. Roussel, *Energy-Aware Object Tracking Algorithm using Heterogeneous Wireless Sensor Networks*, in 4th. IFIP/IEEE Wireless Days, Niagara Falls, Ontario, Canada, October 10-12, 2011.

[3] M. Guerrero-Zapata, R. Zilan, J. M. Barcelo-Ordinas, K. Bicakci, B. Tavli, *The future of security in Wireless Multimedia Sensor Networks : A position paper*, Telecommunication Systems, Vol. 45, Number 1, pp. 77-91, 2010

[4] G. Gaubatz, J.P. Kaps, E. Oztruk, B. Sunar, *Sate of art in ultra-low public key*, in Proc. Of The 2nd IEEE Workshop on Pervasive computing and Communication Security, 2005

[5] R. Watro, D. Kong, S.F. Cuti, C. Gardiner, C. Lynn, 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, Washington, DC, 2004

[6] D. Liu, P. Ning, *Tesla: Broadcast authentication for distributed sensor networks*, Transaction on Embedded Computing Systems, Vol. 3, Number 4, pp. 800-836, 2004

[7] D. Kandris, M. Tsagkaropoulos, I. Politis, A. Tzes, S. Kotsopoulos, *Energy efficient and perceived QoS aware video routing over Wireless Multimedia Sensor Networks*, Ad Hoc Networks, Volume 9, Issue 4, pp. 591-607, 2011

[8] L. Cobo, A. Quintero, S. Pierre, *Ant-based routing for wireless multimedia sensor networks using multiple QoS metrics*, Computer Networks, Volume 54, Issue 17, pp. 2991-3010, 2010

[9] G. A. Spanos and T. B. Maples, *Performance study of a selective encryption scheme for security of networked, real-time video*, In Proc. of the 4th International Conference on Computer Communications and Networks (ICCCN'95), pp. 72-78, Las Vegas, Nevaga, USA, 1995

[10] J. Meyer and F. Gadegast, *Security mechanims for multimedia data with example MPEG-I video*, http://www.cs.tuberlin.de/phade/ hade/secmpeo.html, 1995

[11] R. Lundin, S. Lindskog, *Security Implications of Selective Encryption*, In Proc. of Metric2010, Bilzano-Bozen, Italy, 2010

[12] L. Badia, M. Lindstrom, J. Zander, and M. Zorzi, *An economic model for the radio resource management in multimedia wireless systems*, Computer Communications, vol. 27, no. 11, pp. 1056-1064, 2004. Cognitive Networks," in Proc. of IST Mobile Summit 06, Greece, 2006

[13] A. Rachedi and A. Benslimane, *A secure and resistant architecture against attacks for mobile ad hoc networks*, Security and Communication Network. 3 (2-3). pp. 150-166, 2010

[14] NS2 -Network Simulator, *http://www.isi.edu/nsnam/ns/*

[15] Arvinderpal S. Wander, et al., *Energy analysis of public-key cryptography for wireless sensor network*, http://research.sun.com/projects/crypto

[16] L. Kaddar and A. Mehaoua, *SecVLC : Secure Transmission over Multimedia Wireless Ad Hoc Networks with Energy-awareness*, in Global Information Infrastructure Symposium (GIIS 2009), 2009

[17] D. Vatolin and al., *MSU Video Quality Measurement Tool*, MSU Graphics & Media Lab

[18] Q. Huynh-Thu and M. Ghanbari, *Scope of validity of PSNR in image/video quality assessment*, Electronics Letters 44: 800-801, 2008