A Secure Energy Efficient Schema for Wireless Multimedia Sensor Networks

Nour El Deen M. Khalifa,Mohamed Hamed N. Taha, Hesham N. Elmahdy and Imane A. Saroit

***Abstract*—**Wireless Wireless Sensor Networks (WSNs) have become an important component in our daily lives. In near future, it will dominate the technology industry around the world. WSNs gain its importance due to the variety of vital applications it can participate in such as military, health care, agriculture, surveillance and monitoring natural phenomena applications.WSNs consist of small devices with limited energy and storage capabilities, called sensor nodes. The sensor nodes collect data from physical or environmental phenomena. They cooperatively pass the sensed data through the network to a certain location or sink node where the data can be collected and analyzed.Due to the unprotected nature of wireless communication channels and untrusted transmission medium of WSNs, it becomes vulnerable to many types of security attacks. The attackers ultimately seek to eavesdrop, steal confidential data, injecting false data or even jamming the whole network, so securing these networks becomes a must.In this paper, a proposed security schema for WSNs will be introduced. The proposed security schema will be appropriate for real time multimedia streaming. It will construct its security features within the application and transport layer as the information that the attackers seek ultimately exist within these layers.The proposed security schema consists of two security levels; the first level is encrypting the packet data using Advanced Encryption Standard (AES) while the second level is generating Message Authentication Code (MAC) using Cipher-based Message Authentication Code (CMAC). Both levels achieved the principles of WSNs security and they are (authentication, confidentiality, data integrity and availability).Performance comparisons between the proposed security schema and other security frameworks are presented. Finally, all the presented work in this research was developed and implemented using Network Simulator-2 (NS-2). According to our literature reviews, this research is one of the first researches that use NS-2 as a security simulator. As NS-2 does not support any security features before.[1]

***Keywords*—**Wireless sensor networks, AES, CMAC, Security simulator, NS-2.

I. Introduction

A. Wireless Sensor Networks (WSNs).

A WSN is composed of low cost, low power, multifunctional sensor nodes that are small in size and communicate wirelessly over short distances. WSN can also be introduced as a self configured wireless networks to collect data from physical or environmental phenomena, such as temperature, sound, pressure, motion or pollutants [1]. It cooperatively passes their data through the network to a main location or sink where the data can be monitored and analyzed. A sink node or base station performs like a gate between users and the network.In general, a wireless sensor network may contain hundreds or thousands of sensor nodes. The sensor nodes can communicate among themselves using radio signals. After the deployment of sensor nodes in the monitored area, they are accountable for self organizing an acceptable network infrastructure often with multi-hop communication with each others. Then they start gathering information of interest.

B. Research objectives

The area of WSNs attracts research interest mainly because of their greatly exciting potential. In order to achieve that potential, the research community has to overcome the security obstacle which faces great challenges [2].

Privacy and security is an essential element of many applications in the world. By enabling security in the WSNs, a potential is created to use them for demanding requirements. A well designed security schema is essential for the further development and the success of wireless sensor networks.

The objective of this paper is to provide a secure schema for multimedia streaming in WSNs within the application and transport layer and made the schema as energy efficient as possible. The process of achieving our objectives will be discussed through the paper.

The key challenge in securing sensor networks is how to maximize the lifetime of sensor nodes due to the fact, as it is not feasible to replace the batteries of thousands of sensor nodes. Therefore, computational operations of nodes and communication protocols must be made as efficient as possible in the energy consumption [2].

Among internet protocols, data transmission protocols in application layer have much more importance in terms of energy, since the energy required for data transmission takes 70 % of the total energy consumption of a wireless sensor network [3]. So the process of data transmission should be optimized. This is the second objective of the research, to find a solution to minimize the number of data transmission to make the network energy optimized while adapting the security features we proposed.

II. Security Goals

A sensor network is a special type of ad hoc network. So, it participate some common property as a computer network.

Manuscript received on May 27, 2013.

Nour El Deen M. Khalifa is with the Information Technology Department, Faculty of computers and information, Cairo University, Cairo, Egypt. E-Mail: nourmahmoud@fci-cu.edu.eg

Mohamed Hamed N. Taha is with the Information Technology Department, Faculty of computers and information, Cairo University, Cairo, Egypt. E-Mail: mnasrtaha@fci-cu.edu.eg

Hesham N. Elmahdy is with the Information Technology Department, Faculty of computers and information, Cairo University, Cairo, Egypt. E-Mail: ehesham@fci.cu.edu.eg

Imane A. Saroit is with the Information Technology Department, Faculty of computers and information, Cairo University, Cairo, Egypt. E-Mail: isaroit@fci-cu.edu.eg

Digital Object Identifier No: WC062013001.

The security goals of a wireless sensor network can be classified as follows: [2]

- **Authentication:** As WSN communicates, sensitive data which helps in many important decisions making. The receiver needs to ensure that the data used in any decision-making process originates from the correct source. Similarly, authentication is necessary during the exchange of control information in the network.
- **Integrity:** Data in transit can be changed by the adversaries. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Data integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident.
- **Data Confidentiality:** Applications like surveillance of information, industrial secrets and key distribution need to rely on confidentiality. The standard approach for keeping confidentiality is through the use of encryption.The mechanisms for achieving semantic security will be discussed in more details in section V.
- **Data Freshness:** Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. To ensure that no old messages replayed a time stamp can be added to the packet.

Network energy plays a very important rule in the decision of choosing a security mechanism, thus the following issues should be taken in considerations while designing a security schema: [2]

- **Untethered:** The sensor nodes are not connected to any energy source. They have only a finite source of energy, which must be optimally used for processing and communication. To make optimal use of energy, communication should be minimized as much as possible.
- **Availability:** Sensor nodes may run out of battery power due to excess computation or communication and become unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network.

The above section has discussed the security goals and energy issues that are widely available for wireless sensor networks. The next section explains the attacks that commonly occur on wireless sensor networks.

III. ATTACKS ON WIRELESS SENSOR NETWORKS

Security in any network system does not simply involve only one or two layers, but rather needs to be viewed across all layers as a whole. The security issues for a conventional network differ greatly to the security issues in WSNs because of the extremely limited resources available in sensor nodes. Attacks in the WSN can be categorized into two types, passive and active attacks [4].

- In passive attack, the attacker can get information from WSN by eavesdropping wireless communications and tries to steal confidential data.
- In active attack, the attacker can get information from WSN by spoofing or altering packets in order to breach authenticity of communication or injecting false data to impasse the network.

Attacks could be happened also on different layers of the WSN stack layers. Attacks can be summarized and their security solutions approaches in different layers with respect to WSN layers stack in the Table I. The table presents a classification of various security attacks on each layer of WSN.

TABLE I
LAYERING-BASED ATTACKS AND POSSIBLE SECURITY APPROACH

Layer	Attacks	Security Approach
Application Layer	1. Path-based DoS attack [5] 2. Node Reprogramming attacks [6]	1. Cryptographic Approach 2. Authentication
Transport Layer	1. De-synchronization attack [7] 2. Flooding attack [7]	1. Authentication 2. Complex puzzles [7]
Network Layer	1. Sybil Attack [8] 2. Sinkhole Attack [8] 3. Wormhole Attack [8] 4. Hello flooding attack [8]	1. Three way handshake [9] 2. Authentication 3. Cryptographic Approach
Data Link Layer	1. Collision Attack [10] 2. Interrogation Attack [10] 3. denial of sleep attacks [11]	1. Spread Spectrum techniques [12] 2. Error Correcting Codes[13] 3. Rate control mechanisms[2]
Physical Layer	1. Node Tampering Attack [6] 2. Jamming and Interception Attack [6]	1. Spread Spectrum techniques 2. MAC layer admission [14] 3. Tamper Proofing(camouflaging nodes) [6] 4. Directional antenna for access restriction [15]

In our research, the protocols in the higher layers will be studied in details; the higher layers are the application layer and the transport layer. The reason for choosing higher layers is that the information that the attackers seek ultimately resides within the application layer and its related protocol in transport layer. Attacking directly on both layers makes an impact and reaches the attacker's goals.

A. Transport Layer attacks

The focus of transport layer attacks is to exploit communication protocols that use connection oriented communications and maintain connection information. The main transport layer attacks against WSNs include De-synchronization attacks and Flooding attacks.

- **De-synchronization attack:** an attacker objects active communications and modifies or fakes the parameters of captured messages, such as control flags and sequence numbers. The modified or faked messages are sent back into an active communication stream between two nodes [7]. Consequently, when modified or faked messages

arrive at their respective destinations they are rejected as out of sequence or as corrupted, leading to the sender resending messages and wasting energy and network bandwidth.

The encryption of message headers or the whole message with authentication can ban attackers from modifying existing messages and creating faked packets. Moreover, anti-replay mechanisms [7] can prevent false messages from being inserted into false communication streams undetected.

- **Flooding attack:** The objectives of the attacker are networks employing connection oriented communication protocols. The attacker requests a connection from a node in the WSN; the node detains space in its open connection buffer and sends a synchronization acknowledgement. After a period of time has crossed a timeout counter expires causing the victim to clear its open connection buffer. However, an attacker may repeatedly order a number of connections and leave them half open, exhausting the victim's connection buffer, and preventing false connection requests for the duration of the attack [7]

With the protocols perspective, there are two main protocols in transport layer, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) [16]. In TCP, the attacker make a large number of half opened TCP connections with a receiver node, but never finishes the handshake to fully open up the connection, this will lead to drain in energy.

Another type of attack in TCP is session hijack; the attacker mimics the victim's IP address, determines the correct sequence number that is expected by the target, and then executes a Denial of Service (DoS) attack on the victim node [X]. In order to hijack a session over UPD, the attacker make the same step done in TCP, except that UDP attackers don't need to concern about the overhead of treating sequence numbers and other TCP control fields. Since UDP is connectionless, phasing into a session without being detected is much easier than the TCP [16].

In our research, we will focus on UDP and how to secure it using authentication mechanism and encryption technique which stand against mentioned attacks put will not include flood attacks as it require a special hardware.

B. Application Layer attacks

Attacks targeted at the application layer of WSNs either focus on weaknesses in application software specific to a particular WSN or focus on more general inherent weaknesses in the application layer of WSNs. The most popular forms of application layer attacks include path based DoS attack and Node Reprogramming attack.

- **A path based DoS attack** is an attack on the reliability of the WSN network. An attacker spates counterfeit or replayed packets along a multi hop, end to end routing path. There are a number of methods proposed for defending against path-based DoS attacks, the primary role of most defense approaches is to detect and remove spurious packets along a communication path, there are three generic defense approaches against such attacks [5]:
  1. Each node along a communication path shares a secret key with the sender. The sender generates authentication and integrity material for each key/node and appends it to each packet.
  2. A modified approach, to that discussed in 1, involves a node storing a path key for every potential path in a WSN, if any one of the nodes in the network is subverted an attacker can flood a whole communication path.
  3. Rate control mechanisms can also be applied to each node, limiting the amount of replayed packets accepted from any one node. However, due to the nature of WSN, certain nodes such as nodes directly around a coordinator or router nodes have different packet rates.

- **Node Reprogramming attack,** due to the nature of many WSN applications where nodes are located in inaccessible and remote locations it is desirable to remotely and wirelessly update node software. The process of updating node software is referred to as code dissemination. There are numerous approaches and protocols for disseminating software, such as the approach adopted by TinyOS called Deluge [17]. In the Deluge approach, nodes periodically send advertisements containing their software version.

  Secure methods for reprogramming nodes have emerged, one such scheme is called Seluge [18], a secure extension of the Deluge approach.

With the protocols perspective, the application layer contained user data, and it supported many protocols such as HTTP, SMTP, RTP, and FTP [19], which provide much vulnerability and access points for attackers. As mentioned before preprogramming node attacks (malicious code attacks), such as viruses, worms, spywares, and trojan horses [19], can attack both operating systems and user applications. These malicious programs usually can spread themselves through the network and cause the WSN node and networks to slow down or even damaged.

In our research we focus in the first solution presented in path based DoS attack, using cryptographic approach and add the MAC authentication mechanism. Our research also will focus on the RTP protocol as it commonly used in multimedia streaming.

IV. RELATED WORKS

The WSN security is a mature research area. Data encryption and authentication has been the subject of several research efforts. However, Few Security solutions for wireless sensor networks exist. Most of the current security solutions are developed to be quite general to fit many different platforms and scenarios. The existing security solution deliver security features at the link and network layer Using TinyOS or Contiki operating system. They didn't cover security in application and transport layer together.Common to all of these existing security solutions is that they miss out to consume lower energy and not fitting the real time multimedia streaming. The main related works are TinySec [20],

0974-9756/CIIT-IJ-4479 /03/$20/$100 © 2013CiiT Published by the Coimbatore Institute of Information Technology

MiniSec[21], TinyECC [22] and ContikiSec[23]. They will be compared with the proposed work in the simulation and results section.

Our research may be considered as a base work to researchers to begin to use NS-2 as a security simulator. This research will help the researchers to study the effect of security in energy and other metrics related the WSN such as data rate, packet delivery and packet drop rate... etc. We will discuss in details these metrics in the following sections.

V. The Proposed Schema

A. Design Assumptions

Traffic flow follows a pattern determined by the application. Most of the traffic is assumed to be directed from the nodes to the base station.The reason for that assumption is derived from the ultimate goal of a WSN; to get information from the network.We also assume that all the sensors use integrated circuits that are tamper resistant. Thus, in case a node is captured the attacker is unable to extract data from the sensor especially the networks keys.

Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors).

B. WSN Packet format modifications

The proposed secured packet format was constructed on the current packet format of communication across WSN [Figure 1].

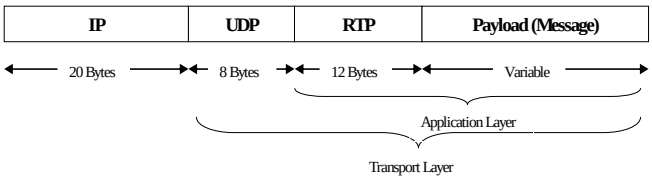

Fig. 1WSN normal packet format

The modifications can be summarized by the following points [Figure 2]:

- Payload encryption using symmetric encryption algorithm.
- Generating Message Authentication Codes (MAC) code using encrypted payload, RTP header and UDP header. The generated code will be stored in MAC header field (4 bytes).

A new PassWord (PW) filed had been added to the proposed secured schema. The PW filed hold 2 bits and it would contain the following values {00, 01, 10, and 11}. The values of PW would notify the secured schema which key password would be used to encrypt and decrypted the payload. The PW field made the proposed security schema more computationally secured against known attacks other than any solutions for security.

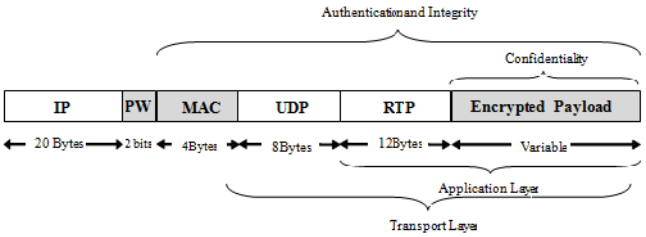

Fig. 2 Proposed secured packet format for WSN

By applying the previous two mechanisms, our research achieved four goals of six security goals mentioned in section II. The achieved four goals are data authentication, integrity, confidentiality and freshness which are achieved by using sequence number field in RTP header [24].

C. Symmetric Encryption

The Advanced Encryption Standard (AES) [25] encryption was selected in our proposed schema for its security properties and for its powerful mechanism which stand against well known attacks and suits variable plaintext lengths.

Although we believe that AES is the most suitable for use in WSNs, there are no security risks in using any other encryption function with our schema. The features of AES algorithm have been investigated and its effect on energy has been studied well in researches [26] [27]. Both researches included that AES is the most suitable encryption algorithm for WSN according to energy metric.

D. Message authentication codes (MAC).

A common solution for achieving message authenticity and integrity is to use a message authentication code. A MAC can be viewed as a cryptographically secure checksum of a message.

Computing a MAC requires authorized senders and receivers to share a secret key, and this key is part of the input to a MAC computation. The sender computes a MAC over the packet with the secret key and includes the MAC with the packet.

We authenticate our data by adding CMAC code [28]. Such code is generally a small amount of data appended in the end of the packet.

CMAC is a block cipher-based message authentication code algorithm. It is used to provide assurance of the authenticity and, hence, the integrity of data. This mode of operation fixes security deficiencies of CBC-MAC [29] (CBC-MAC is secure only for fixed-length messages).

E. Proposed Security Schema Design.

Multimedia streaming is quite different form message transmission across wireless sensor network. The difference can be itemized by the following points:

1. Large data size (frame size varying from 1000 to 3000 bytes).

2. The real time characteristic (frames should be sent and received in a bounded delay)
3. Video should be sent in a certain frame rate (standard 24 frame per second)
4. Energy consumed by sensors should be taken into consideration while sending and receiving frames.

The above points made any proposed security mechanism was very hard to be implemented. We overcome these problems by:

1. Fit the video frame in the standard frame size for RTP multimedia streaming. The standard frame size will be 1536 bytes and frame height and width would be 352x288 pixels.
2. Sizing the video frame in the standard format, made us execute AES and CMAC on the video frame, and we found that both algorithms can fit multimedia streaming
3. Proposing a multimedia scheduler which made a significant save in the consumed energy by discarding frames that can't burden the process of encryption, decryption and authentication by the video camera sender node.

Figure 3 represent the send function of the proposed security schema for multimedia streaming.

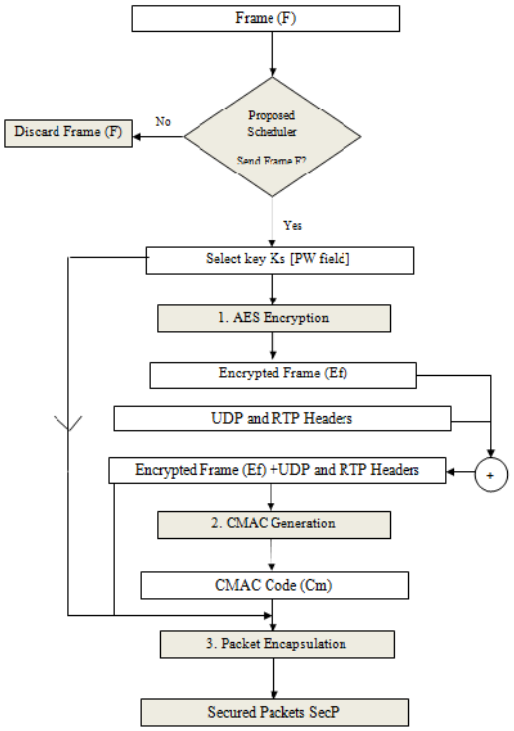

Fig. 3Sent function for the proposed security schema

A frame could be lost by three reasons in the proposed security schema for multimedia transmission:

1. Due to encryption process by the sender node as a new frame need to be sent while encrypting the current frame.
2. Due to decryption process in the receiver node as a new frame need to be displayed while decrypting the current frame.
3. Due to network traffic congestion.

The proposed multimedia scheduler discard frame by the sender node from the beginning according to the following process as illustrated in figure 4:

1. Initialize the time of encryption, decryption and authentication as T_{ENC} , T_{DEC} and T_{AUTH}
2. Calculate time needed to secure a frame {$T_{SEC} = T_{ENC} + T_{DEC} + T_{AUTH}$}
3. Buffer two frame frameA and frameB and calculate the time between them as T_{AB}
4. If $T_{AB} > T_{SEC}$ then scheduler pass frameA to the proposed security schema else discard frameA and continue until the end of all video frames.

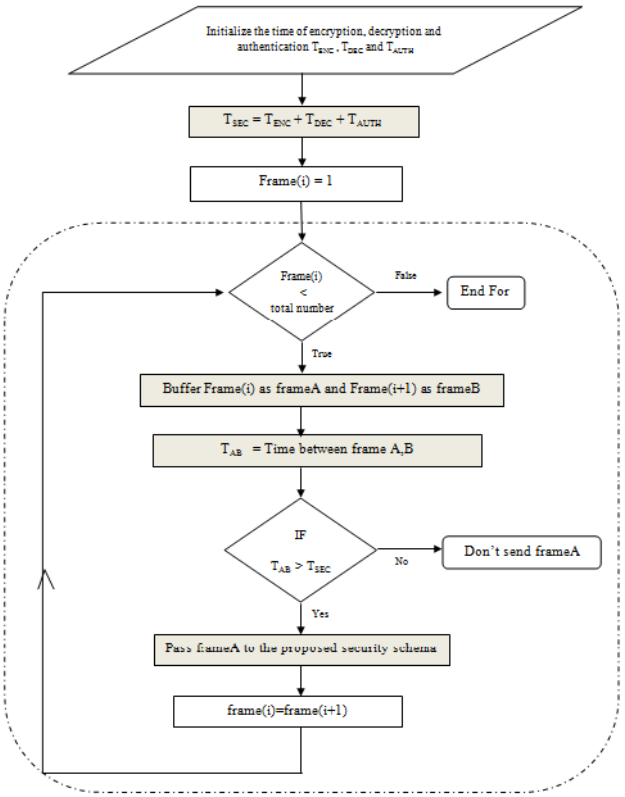

Fig. 4 Proposed security scheduler for multimedia streaming

For example if T_{SEC} is equal to 40 milliseconds and the time between frame A and B is 42 milliseconds, then T_{AB} is greater

than T_{SEC}, so frame A would be secured and sent across the network to receiver node; else the frame would be discarded by sender (video camera sensor). Figure 5 illustrates the process of Receive function for the proposed security schema

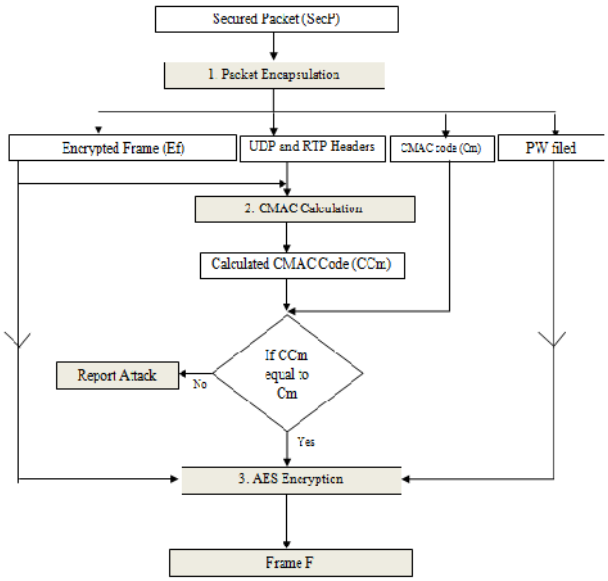

Fig. 5 Receive function for the proposed security schema

F. Implementation Details.

Ns-2 is an object-oriented simulator developed as part of the VINT project at the University of California in Berkeley [30]. Ns-2 is extensively used by the networking research community. It provides substantial support for simulation of TCP, UDP, routing, multicast protocols over wired and wireless (local and satellite) networks, etc. [30]

NS-2 doesn't support any security module before, but the research succeeded to build a core package to add security features in NS-2. Figure 6 illustrates the "EvalVid" tool that can be integrated with NS2 to send a real time multimedia streaming over WSN and proposed by Chih-Heng [31]

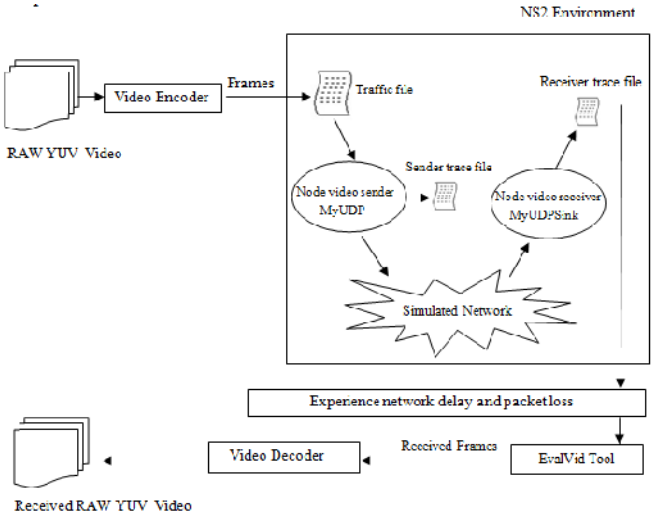

Fig. 6 Design diagram of EvalVid tool proposed by Chih-Heng

A security library (Crypto++)[32] has been integrated with NS2 and EvalVid Tool. Crypto ++ is a free and open source C++ class library of cryptographic algorithms such as AES, DES, HMAC, CMAC..etc

The secured packet format has been implemented to adapt the changesas illustrated in [Figure 2] (application layer modification). Figure 7 illustrates the modification done to EvalVid tool to adapt our security schema.

G. Experiments Data

The researchers of this work used the standard videos sequences that commonly used for multimedia experiments. The videos sequences can be found in the website http://trace.eas.asu.edu/yuv/index.html [33]. Figure 8 illustrates both videos used in the simulations scenarios

Fig. 8 Screenshots for videos used in research experiments

ffmpeg" [34] encoder had been used to convert video files to MPEG format. The encoder "ffmpeg" is cross-platform solution to record, convert and stream audio and video files.. After converting files into MPEG format, these file are used in NS2 simulation. One frame example used in NS2 is presented in figure 9.

1364566535.613739 RTP len=1328 from=193.227.14.69:1728 v=2 p=0 x=0 cc=0 m=0 pt=33 (MP2T,0,90000) seq=17574 ts=764884950 ssrc=0x6062
data=4700441830087810a0009804c3d84267041160107 03e9049fd900d8a0244f862eeb0 03f01593a0007a50c01288ae0411600b80250d049fd4cdc01a006408bf64d008fc005881d0 05ee9c031cc01381c814027703f6904114010022fe10c2d31c00f085ba920549f303081d30 980000010713e5210422804a3cc48fab014013482481a6ee003d040b1006201a00c434988 210064a4f3c0a61f5a0835000ac1141803004907d2d17e6f13099c113e90149204b8040189 044fac0112481470044197a5041aa005608a0a01802484620cc9040ac005690440400d038 990a1f17e601046807430349a58150c28a2b3a529417941f7ad040d7040d42804f8004c00f 1001600645125949018960 4cb01e0ed6e006e081a400cc01993124202a02748184a5c0c21 58408badeaef4e50eba48403be4c2186135868182d09183dbdf37e08168008007690074031 417c06e42e05c0744d412908ecce064e55f4e1b177a9242259b3e5fbf98940819800c099c 04e3001b809834033010ac4700441a9a03b4b801f00e8ac480c267602e330042bbaa00560 818801860070082280 0b121a1a4b700ac04e9412897d20391802b235ee33dc704033005c9 004a00ac040030f8050349658e1852e8298999440b6e0302596352bbf0c0805600a000480 0c004c3402726e01b96028dcf38fb9a4a1860250222c65f410821999590 72b5a8b00cc0748 5a58127f711a961a6d992156e91a4dc089f480152a24c00b4306e042fa2dc09e7fa2083c80 191c84164d141986ca5006a0310d01c4700441b00605958796 96f0103f43fba09a4221931 01890094c199c3eb0964300903412 40f55621a4602182963620169340 90c81904bf6ee054 706856a380c4090693aac9658fab2b00f644a912eef03203b024980d01df3135092600f665 231a1704a9819bb98863933701b8e485d512f80484fa604704c170062097768217b8e0b4c a4a013869e4eaa74a4908d40321b80fcc95036e200749412406fc412a54908998117f00236 0595879696f0103f43fba09a422193101890094c1996059587969 6f0103f43fba0605958

Fig. 9 An example of frame to be sent by a node in multimedia streaming scenario

VI. Simulations And Results

This section will be divided into three sections, the first section will present the NS2 simulation parameters while the second parameters will present the performance metric, in the

third section simulation results will be introduced with a comparison with other related works.

A. Simulation Parameters

This section illustrates the NS2 simulation parameters to be carried out through simulation scenarios. A brief overview of the NS-2 simulation parameters is presented as shown in table II.

TABLE II
SIMULATION PARAMETERS

Simulation Parameters	Values
Mac Layer Protocol	IEEE 802.11
Transmission Radius	250 M
Data Rate	24 frame/sec
Traffic Type	Multimedia Frame
Simulation Area	1000m x 1000m
Number of Sensor Nodes	25
Node Initial Energy	1000 J
Transmission Energy	0.007 J
Reception Energy	0.007 J
Simulation Times	120 sec
Routing Protocols	AODV

There were 4 scenarios in multimedia streaming, when a 1, 2, 3 and 4 video cameras existed in the network topology with different positions. The metrics to be measured were the total network consumed energy, network packet delivery ratio and Peak Signal to Noise Ratio (PSNR).

B. Experiments Metrics

The Total network consumed energy is defined as the summation of energy consumed by every node in the network during a specific time. Equation 1 is used to calculate the total network consumed energy.

$$Total\ network\ consumed\ energy = \sum_{i=1}^{n} E_i \quad (1)$$

Where:
n represents total number of nodes.
E_i represents the consumed energy by node *i*.

The Network delivery ratio is defined as the number of successful received packets during a specific time. Equation 2 is used to calculate the network delivery ratio.

$$Network\ delivery\ ratio = \frac{\sum_{i=1}^{n} RP_i}{All\ Transmitted\ Packets} \quad (2)$$

Where:
n represents the total number of nodes.
RP_irepresents the received packets by node *i*.

PSNR is defined as the normalized average difference between each pixel in the transmitted video and the received video through the network. This is the most commonly used method to measure video quality. Equation 3 and 4 is used to calculate PSNR.

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} \quad (3)$$

$$MSE = \frac{1}{N \square M} \sum_{i-0}^{N-1} \sum_{j=0}^{M-1} [X(i,j) - Y(i,j)]^2 \quad (4)$$

Where:

L represents the maximum value a pixel can take in a video frame.
MSE represents the Mean Square Error.
X represents the transmitted video frame.
Y represents the received video frame.
i,j represent the location of the pixel in a video frame

C. Experiments Results

The first metric to be measured through the proposed work was the total network consumed energy. Figure 10, figure 11, figure 12 and figure 13 represents the consumed energy by the network when there are one, two, three and four videos streamed through the network consequently. The X axis represents the location of the video cameras while the Y axis represents the network consumed energy in Joules.

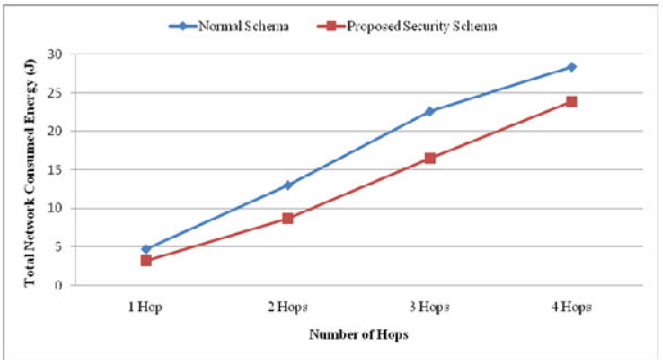

Fig. 10 The network consumed energy for a one streamed video

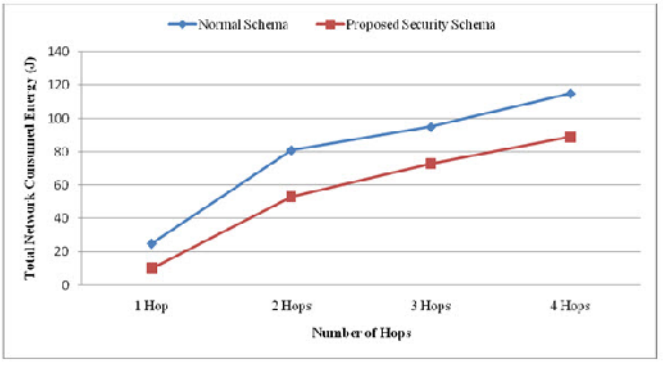

Fig. 11 The network consumed energy for two streamed videos

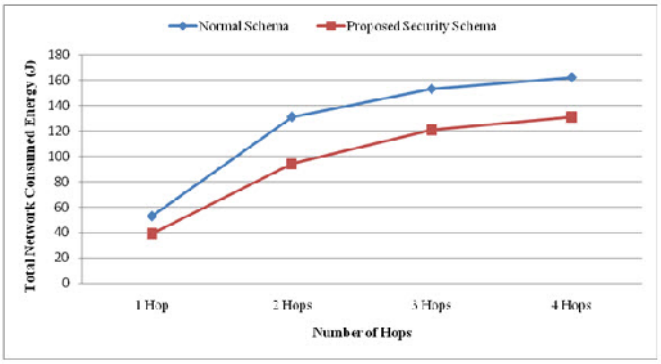

Fig. 12 The network consumed energy for three streamed videos

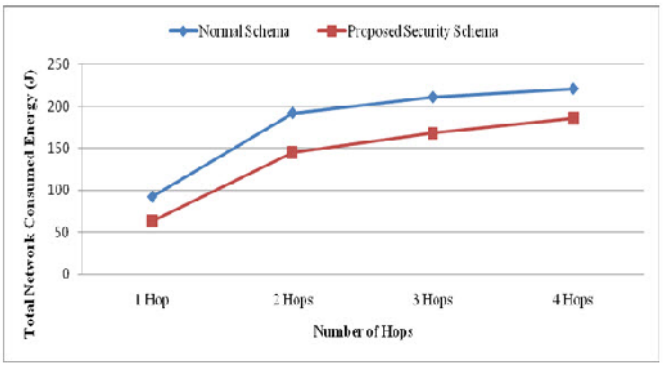

Fig. 13 The network consumed energy for four streamed videos

From figure 10 to figure 13 illustrated that the proposed security schema achieved less energy consumption than the normal schema. The proposed scheduler achieved this improvement in the network consumed energy. The video camera sensor would discard any frame that would not burden the process of encryption, decryption and authentication before sending it to their destination. This idea conserved a lot of consumed energy as there were frames that were going to consume a lot of energy through its journey to the sink node and when it reached the sink node, it would be dropped as it couldn't burden the process of decryption. The consumed energy through its journey was proportional to the video camera location, the far the video camera located the more energy the frame consumed to reach the sink node.

The question might be asked in this part, what were the times when two, three and four video streamed through the network. If the two, three or four videos were been streamed and there was a pause time between them, then there wouldn't be a problem as the network would handle this situation as there was a one video at time.

A random start times for videos were generated. The random time would be generated according to uniform distribution. The uniform distribution would generate two numbers between 0 and 40 in case of two video streamed through the network. The value 40 was the result of multiplied the duration of the movie by the number of videos to be streamed. In case of three videos, the random times to start streaming would be between 0 and 60… etc.

The simulations were executed 10 times for every scenario and the average was calculated from these values to draw the figure for the network consumed energy and the other metrics.

The second metric to be measured through the proposed work was the total network delivery ratio. Figure 14, figure 15, figure 16 and figure 17 represents the network delivery ratio when there are one, two, three and four videos streamed through the network consequently. The X axis represents the location of the video cameras while the Y axis represents the achieved network delivery ratio in percentage.

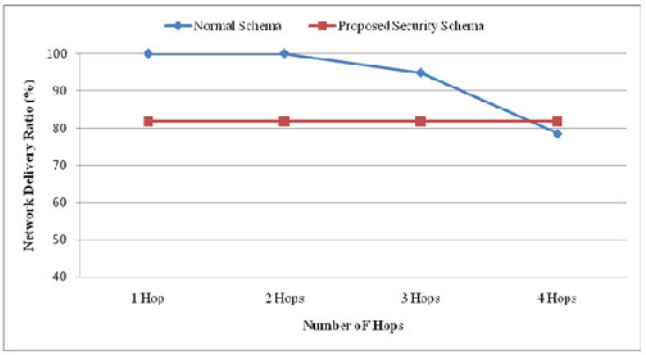

Fig. 14 The network delivery ratio for one streamed video

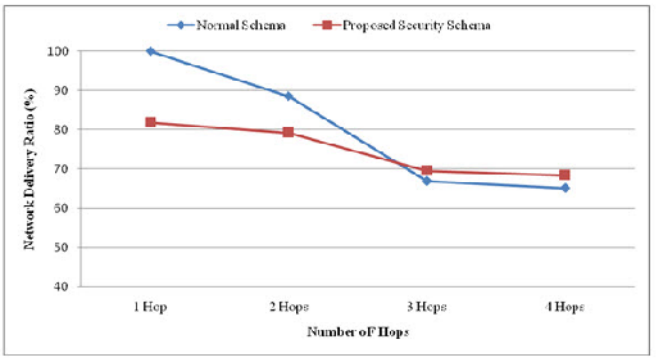

Fig. 15 The network delivery ratio for two streamed videos

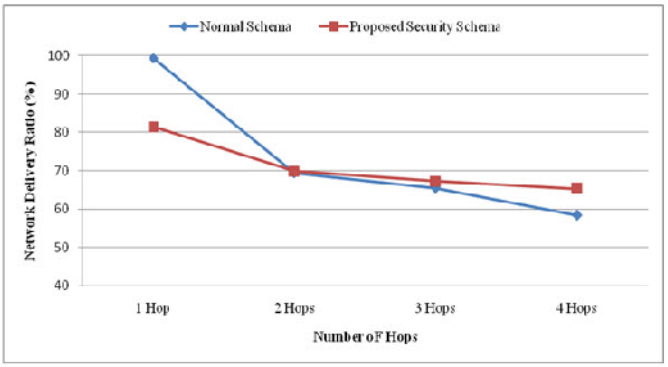

Fig. 16 The network delivery ratio for three streamed videos

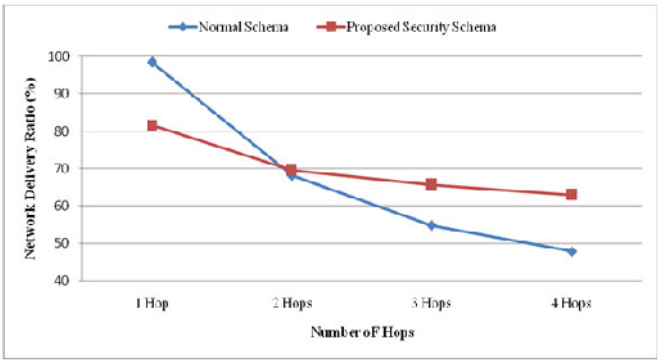

Fig. 17 The network delivery ratio for four streamed videos

Figure 14 illustrated that the proposed security schema delivery ratio was 81%. The 81% delivery ratio achieved due to the discarded frames by the proposed scheduler. When the video camera was away from the sink by 4 hops, the delivery ratio of the normal schema was below 81% while the proposed secured schema is constant at 81%. The normal schema delivery ratio was below 81% due to network traffic congestion.

From figure 15 to figure 17 clarified that the delivery ratio of the proposed secured schema was not constant at 81% likewhen there was one video streamed through the network. The delivery ratio of the proposed security schema was below 81%. The reason for that phenomenon was the network traffic congestion as there were two, three and four video cameras and their locations were away from the sink by 2, 3 and 4 hops.

For multimedia streaming, the video was considered in a good quality to be watched when no more 1/3 of frames were being lost. The proposed secured schema and the normal schema achieved more than 65% delivery ratio as illustrated in figure 14 to figure 16, which was a good indicator for movie quality. PSNR would strength our indication at the end of multimedia results section.

Note that, in figure 17 at 4 hops away from the sink node, the delivery ratio of the normal schema and the proposed secured schema was below 65%. This value was not acceptable for video quality. But this case was the worst case scenario would be happen in the whole simulations scenarios. Thus a random deployment for videos cameras was required to draw the final conclusion of the proposed security schema performance. The PSNR would also have the final decision about the quality of the streamed videos.

PSNR metric had to be calculated for every video streamed through the network with every simulation scenario. About 112 PSNR graph should be illustrated through this research, but the researcher decided to calculate the PSNR when the worst delivery ratio achieved in the network. The worst delivery ratio happened when 4 videos to be streamed through the network, and there were 4 hops way from the sink. The delivery ratio was 62 %. Figure 18 illustrates the PSNR graph when worst case occurred during the simulations.

The achieved PSNR mean value was 20.43 db. This value was quite low but acceptable, as the accepted region for PSNR value was between 20 – 25 db for wireless transmission. The achieved PSNR indicated that the proposed security schema for multimedia streaming not only achieved less energy consumption but also achieved acceptable delivery and PSNR value while proposing a strong security schema (4 times stronger than any proposed security schemas) .

Table III introduces performance comparisons between the proposed security schema and other related work. The proposed security schema works within transport and applications while other related works operate in link and network layer. the proposed security schema is stronger 4 time and have acceptable overhead and support multimedia while other related work don't support multimedia according to the literature reviews.

TABLE III
PERFORMANCE COMPARISONS BETWEEN PROPOSED SECURITY SCHEMA AND OTHER RELATED

Framework Name	Year	Implemented/ Simulated	Security Properties	Algorithms	Layer	Overhead	Key length	Support Multimedia
TinySec[20]	2004	Implemented (NesC)	Access Control, Integrity, Confidentiality, Replay Protection	Skipjack CBC-CS mode	Link Layer	8 bytes/packet	80	-
SenSec[35]	2005	Implemented (NesC)	Access Control, Integrity, Confidentiality, Key Management	Skipjack-X CBC-CS mode	Link Layer	5 bytes/packet	80	-
MiniSec[21]	2007	Implemented (NesC)	Pre-Deployed symmetric keys, Confidentiality, Replay Protection, authentication	Skipjack OCB mode	Network layer	3 bytes/packet	80	-
TinyECC[22]	2007	Implemented (NesC)	Key Exchange, Public key encryption, Digital signature	ECC SECG-160	Link Layer	Keys overheads	256	-
ContikiSec[23]	2009	Implemented (C)	Authentication, Integrity & Confidentiality	AES CBC-CS mode	Network Layer	4 bytes/packet	128	-
Proposed Security Schema	2013	Simulated (NS2 - C)	Authentication, Integrity, Confidentiality & freshness	AES CMAC mode	Transport and Application layer	4 bytes/packet + 2 bits/packet	256 – 4 times stronger than TinyECC	Yes

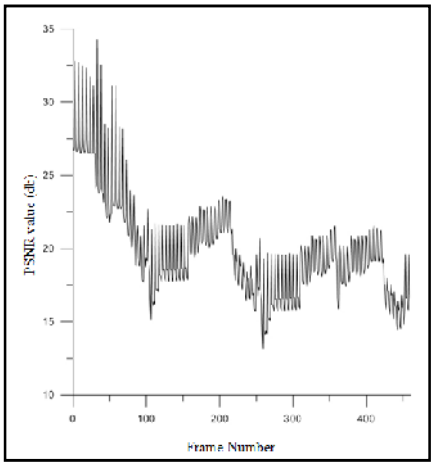

Fig. 18 PSNR between the original video file and the received video file with the worst case scenario

The proposed security schema for multimedia streaming results through the previous sections had been proved its effectiveness against the normal schema. The effectiveness of the proposed security schema was been measured and tested against the normal schema according to three metrics. The metrics were the energy consumption, network delivery ratio and PSNR.

The proposed security schema for multimedia streaming had advantages and disadvantages, the forthcoming points would illustrate the advantages of the proposed security schema for multimedia streaming:

1. The proposed security schema added security features to WMSN and 4 times stronger than any proposed security schemas.
2. Although the proposed security schema added security features to WMSN, it achieved less energy consumption due to the proposed scheduler.
3. It achieved acceptable delivery ratio when video camera are deployed away from the sink node.
4. In the worst case scenario although the proposed security achieved a delivery ratio 62% but PSNR illustrated that the video subjective quality was acceptable and achieved 20.43 db
5. The far the video cameras are deployed; the better results the delivery ratio would be achieved by the proposed security schema.
6. The decision of selecting how many sensor cameras would be deployed and where to deploy them would be a network engineer design parameter.

The proposed security schema for multimedia streaming had also a set of disadvantages and they were:

1. The proposed security schema had achieved less delivery ratio than the normal schema when the network always had only one video camera deployed in the network.
2. It had also a less delivery ratio than the normal schema when video cameras are deployed in a 1 hop away from the sink node.

VII. Security analysis

Any proposed security schema is claimed to be computationally secure if it could withstand the following two criteria. Firstly, the cost of breaking the cipher should exceed the actual value of the encrypted information. Secondly, the time required to break the cipher should exceed the useful lifetime of the information.

The proposed security schema satisfies both the criteria. The CMAC authentication mechanism prevents by default a lot of attacks which were mentioned in section II. The security strength of the AES encryption would be checked against ciphertext only attack, known plaintext attack as these were the most important attacks [25].

The AES encryption with key size 256 bit (32 bytes), the attacker in ciphertext only attack should monitor 2^{32} cipher texts while in known plaintext attack should try 2^{256} key combination.

With the use of massively parallel organizations of microprocessors, it might be possible to achieve processing rates many orders of magnitude greater. If a system that can process 1 million keys per microsecond the AES with key size 256, it would consume 2^{255}ms equal 5.7×10^{42} years. The proposed 4 password to be used through the proposed schema, made the proposed schema even more computationally secured.

VIII. Conclusions

This research has introduced a security schema for multimedia streaming in Wireless Sensor Networks. This research has shown that how the proposed schema has achieved the security goals and issues, and how it has operated. The proposed schema has been compared with other existing schemas that share common goals.

The proposed schemaworks within the application and transport layer using AES encryption algorithm and CMAC message authentication. It was implemented using NS-2.According to our literatures reviews, this research can be considered as one of the first researches that have succeeded to add security features in NS-2.

IX. Future works

The presented security schema is almost complete but there is always room for improvements. A potential future version could include a modification on RTP to reduce the data overhead by removing the destination address of sink node as all nodes sends data to sink node.

Another potential future research is to implement the proposed work in WSN operating systems and compare it with existing related works.

0974-9756/CIIT-IJ-4479 /03/$20/$100 © 2013CiiT Published by the Coimbatore Institute of Information Technology

X. REFERENCES

[1]. I. F. Akyildiz and M. C. Vuran, “Wireless Sensor Networks”, First edition, John Wiley and Sons Publication 2010.

[2]. J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor Network Security: A Survey", Book chapter in Security of Distributed, Grid, and Pervasive Computing, CRC Press, pp.374-410, 2007.

[3]. S. Bala, “Secure Routing in Wireless Sensor Networks”, Master thesis, Computer and engineering department, Thapar university, May 2009.

[4]. S. Prasanna and S. Rao, “An Overview of Wireless Sensor Networks Applications and Security”, International Journal of Soft Computing and Engineering , vol. 2, no. 2, pp. 2231-2307, May 2012.

[5]. J. Deng, R. Han and S. Mishra, “Defending against path-based DoS attacks in wireless sensor networks”, The Third ACM Conference on Security of Ad hoc and Sensor Networks, New York, USA, pp. 89–96, November 2005

[6]. E. Cayirci, and C. Rong, “Security in Wireless Ad Hoc and Sensor Networks”, First edition, John Wiley and Sons Publication 2009.

[7]. V. P. Singh, S. Jain and J. Singhai, “Hello Flood Attack and its Countermeasures in Wireless Sensor Networks”, International Journal of Computer Science Issues, vol.7, no.11, pp. 23-27, May 2010

[8]. C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and Countermeasures”, Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 3, pp. 293-315, May 2003

[9]. J-H. Huang , J. Buckingham and R. Han, “A Level Key Infrastructure for Secure and Efficient Group Communication in Wireless Sensor Network”, First International Conference on Security and Privacy for Emerging Areas in Communications Networks, Athens, Greece, pp.249-260, September 2005

[10]. SH. Mohammadi and H. Jadidoleslamy, “A Comparison of link layer attacks on wireless sensor networks”, International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks, vol.3, no.1, pp. 69-84, March 2011.

[11]. M. Brownfield, G. Yatharth, et al., "Wireless Sensor Network Denial of Sleep Attack," in the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, New York, USA, pp. 356–364, June 2005.

[12]. A. Rgheff and M. Ali “Fundamentals of spread-spectrum techniques”, 2007. Last accessed on May 2013. http://v5.books.elsevier.com/bookscat/samples/9780750652520/9780750652520.pdf

[13]. M. R. Islam, “Error Correction Codes in Wireless Sensor Network: An Energy Aware approach”, International Journal of Computer and Information Engineering, vol. 4, no. 1, pp. 59-64, August 2010.

[14]. M. Li and B. Prabhakaran, “MAC Layer Admission Control and Priority Re-allocation for Handling QoS Guarantees in Non-cooperativeWireless LANs”, Mobile networks and applications, vol. 10, no.6, pp. 947-959, October 2005.

[15]. J. Cho, J. Lee, T. Kwon, and Y. Choi, “Directional antenna at sink (daas) to prolong network lifetime in wireless sensor networks”, Twelve European Wireless Conference for Enabling Technologies on Wireless Multimedia Communications, Athens, Greece, pp. 1-5, April 2006.

[16]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, vol.40, no.8, pp. 102- 114, August 2002.

[17]. J. Hue, "Deluge 2.0-tinyos network programming", 2005. Last Accessed on May 2013. http://www.cs.berkeley.edu/jwhui/research/deluge/deluge-manual.pdf

[18]. S. Hyun , P. Ning , A. Liu , W. Du,” Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks”, Seventh International Conference on Information Processing in Sensor Networks, New York, USA, p.445-456, April 2008

[19]. A. K. Pathan, “Security of self-organizing networks: MANET, WSN, WMN, VANET”, First edition, Auerbach Publication 2010.

[20]. C. Karlof, N. Sastry, and D. Wagner, “Tinysec: a link layer security architecture for wireless sensor networks”, The second international conference on Embedded networked sensor systems, New York, USA, pp. 162–175, November 2004.

[21]. M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "MiniSec: A Secure Sensor Network Communication Architecture", The Sixth International Conference on Information Processing in Sensor Networks, Massachusetts, USA, pp.479-488, April 2007.

[22]. A. Liu and P. Ning, “TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks”. Technical Report TR-2007-36, Department of Computer Science, North Carolina State University, November 2007.

[23]. L. Casado and P. Tsigas, “Contikisec: A secure network layer for wireless sensor networks under the contiki operating system”, Fourteen Nordic Conference on Secure IT Systems, Oslo, Norway, pp.133–147, October 2009.

[24]. H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, “RFC 1889 – RTP: a transport protocol for Real-Time applications,” Internet Engineering Task Force, January 1996.

[25]. W. Stallings, “Cryptography and Network Security”, Fourth Edition, Prentice Hall 2006.

[26]. J. Lee, K. Kapitanova and SH. Son, “The Price of Security in Wireless Sensor Networks,” Computer Networks, vol.54, no.17, pp. 2967-2978, December 2010

[27]. Y. Wang, G. Attebur and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” IEEE Communications Surveys and Tutorials, vol. 8, no. 2, pp. 2-23, April 2006.

[28]. R. Yasmin, “An efficient authentication framework for wireless sensor networks”, Doctorial Thesis, College of Engineering and Physical Sciences, The University of Birmingham, November 2012.

[29]. J. Black and P. Rogaway, "CBC MACs for Arbitrary- Length Messages: The Three-Key Constructions", Journal of Cryptology, vol. 18, no. 2, pp. 111-132, spring 2005

[30]. Vint Project, “The Network Simulator - ns-2”, 1989, Last Accessed on May 2013. http://www.isi.edu/nsnam/ns/

[31]. K. Chih-Heng, “EvalVid : an evaluation tool-set which do realistic simulation for video streaming”,2008 , Last Accessed on May 2013. http://140.116.164.80/~yufrank/YCY/myevalvid_rtp.htm

[32]. D. Bider, “Crypto ++ library”, 2007, Last Accessed on May 2013. http://www.cryptopp.com/

[33]. National Science Foundation, Arizona State University, “YUV Video Sequences datasets”, 2000, Last Accessed on May 2013. http://trace.eas.asu.edu/yuv/

[34]. F. Bellard, “FFmpeg: software to record, convert and stream audio and video”, 2004, Last Accessed on May 2013. http://www.ffmpeg.org/

[35]. L. Tieyan, W. Hongjun, W. Xinkai and B. Feng, “SenSec Design, Sensor Network Flagship Project”; Technical Report TR v1.0, InfoComm Security Department, Institute for Infocomm Research in Singapore, February 2005.

Nour El Deen M. Khalifa received his B.Sc. in Computer Science from the Faculty of Computers and Information, Cairo University, Cairo, Egypt in 2006. He received his M. Sc. in Computer Science from the same university in2009. He is working toward his Ph. D degree. His researches are focused on computer networks, wireless sensor networks and security. E-mail: nourmahmoud@fci-cu.edu.eg.

Mohamed Hamed N. Tahareceived his B.Sc. in Computer Science from the Faculty of Computers and Information, Cairo University, Cairo, Egypt in 2006. He received his M. Sc. in Computer Science from the Department of Information Technology,Faculty of Computers and Information, Cairo University in2009. He is working toward his Ph. D degree. His researches are focused on computer networks, wireless sensor networks and quality of service. E-mail: mnasrtaha@fci-cu.edu.eg

Prof. Hesham N. Elmahdy is a professor at the Information Technology Department in Faculty of Computers and Information, Cairo University. He received his B.Sc. in Automobile Engineering with honor degree in the Military Technical Collage, Cairo in 1981. He received his first M. Sc. in Computer Science in the Institute of Statistical Studies & Research, Cairo University, Cairo in 1992. He received his second M.Sc. in Computer Science in the University of Mississippi in August 1996. He received his Ph D in Computer Science in the University of Mississippi in December 1997. His current research interests are Networks, Distance Learning, and Multimedia. E-mail: ehesham@fci-cu.edu.eg

Prof. Imane A. Saroit received her B. Sc. In 1985, M. Sc. in 1990, and the Ph. D in 1994 all from Faculty of engineering, Communication department, Cairo University. She worked in Cairo university since 1989, She is now a professor in Information Technology department and Vice dean for Education and Student Affairs, Faculty of Computers and Information, Cairo University. Her researches are focused on computer networks, specially wireless and mobile networks E-mail: i.saroit@fci-cu.edu.eg