A Secure Energy Mechanism for WSN and Its Implementation in NS-2

Nour El Din M. Khalifa, Mohamed H. Taha, Hesham N. Elmahdy and Imane A. Saroit

***Abstract*—**Wireless sensor networks (WSNs) are usually deployed for gathering data from unattended or hostile environments. Therefore, securing data transmission across these environments is a must. Due to the fact that the sensors have a limited power, any security mechanism for sensor network must be energy efficient. In this paper, a secure energy efficient mechanism is introduced with a proposed scenario which leads to a significant improvement in network energy consumption. The mechanism constructs its security features in the application and transport layer as the information that the attackers seek ultimately resides within these layers. We modified the packet format for WSN. Data payload was encrypted by Advanced Encryption Standard (AES) and Message Authentication Code (MAC) was generated to assure data confidentiality and integrity. The energy consumption metric has been taken into considerations while designing and testing the mechanism to make it energy efficient as much as possible. The energy efficiency was achieved by giving a higher priority to the secured packet over the normal packet in the Interface Queue (IFQ). Through this paper, a detailed structure of the proposed mechanism is introduced and implemented using Network Simulator-2 (NS-2). This is the first research that implements security algorithms within NS-2. Since NS-2 does not support any security features before, this research will be a good start to begin using NS-2 as a security simulator.

***Keywords*—**Wireless sensor networks, Security, Encryption, AES, MAC, NS-2, IFQ.

I. INTRODUCTION

A. *Wireless Sensor Networks (WSNs).*

A typical Wireless Sensor Networks (WSNs) are consisting of a large number of low cost, low power, and multifunctional sensor nodes that are deployed in a region of interest. These sensors may have wireless communications and computing capabilities. They are small in size, but are equipped with sensors, embedded microprocessors and radio transceivers. Sensor nodes are scattered in an unattended environment (i.e. sensing field) to sense the physical world. They communicate over a short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, battlefield surveillance, and industrial process control. Sensed data can be collected by small number sink nodes which have accesses to infrastructure networks like the internet. The deployment nature of sensor networks made it prone to physical interaction with environment and resource limitations raises some serious questions to secure these nodes against adversaries [1].

B. *Research objective*

The area of WSNs attracts considerable research interest mainly because their greatly exciting potential. In order to achieve that potential, the research community has to overcome the security obstacle which poses great challenges [1].

Privacy and security is an essential element of many applications in the world. By enabling security in the WSNs, we create the potential of using them for demanding requirements. A well designed security mechanism is essential for the further development and the success of wireless sensor networks.

The objective of this paper is to provide an efficient and secure energy mechanism for WSNs. 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, that 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.

Among these 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 [2]. So for maximizing the network lifetime, the process of data transmission should be optimized. The data transmission can be optimized by using efficient mechanism, which we introduce in this paper.

II. SECURITY GOALS AND ENERGY ISSUES

A sensor network is a special type of ad hoc network. So, it participate some common property as a computer network. The security goals of a wireless sensor network can be classified as follows: [1]

Manuscript received on December 12, 2012.

Nour El Din 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 H. 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: i.saroit@fci-cu.edu.eg

Digital Object Identifier No: WC122012009.

• 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 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. We will discuss mechanisms for achieving semantic security in more detail 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.

The issues related to sensor network energy play 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 mechanism: [3]

• 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 SENSOR NETWORKS

Attacks can be classified into two major categories for wireless sensors networks, according the interruption of communication act, namely passive attacks and active attacks. From this regard, when it is referred to a passive attack it is said that the attack obtain data exchanged in the network without interrupting the communication. When it is referred to an active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network, meaning information interruption, modification, or fabrication.

Examples of passive attacks [1] are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

Attacks could be happened also on different layers of the internet model. Although there is no such standard layered architecture of the communication protocol for wireless sensor network, attacks can be summarized and their security solution approaches in different layers with respect to ISO OSI layers [1] in the Table I. The table presents a classification of various security attacks on each layer of the internet model.

In our research, we will focus on the higher protocol layers in the ISO OSI architecture, which is transport and application 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.

TABLE I
LAYERING-BASED ATTACKS AND POSSIBLE SECURITY APPROACH

AODV packet type	Attacks	Security Approach
Application Layer	Attacks on Reliability, Repudiation and data corruption	Cryptographic approach
Transport Layer	injects false messages and energy drain attacks	Authentication
Network Layer	Packet drop, Wormhole, blackhole, flooding, resource consumption [1]	Authentication
Data Link Layer	Jamming and collision [4]	Use error correcting codes and spread spectrum techniques
Physical Layer	Jamming, interceptions and Eavesdropping [5]	Use spread-spectrum techniques and MAC layer admission control mechanisms

A. Transport Layer attacks

The objectives of transport layer protocols in WSN include setting up of end-to-end connection, end to end reliable delivery of packets, flow control, congestion control, and clearing of end-to-end connection.

There are two main protocols in transport layer, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) [6]. In TCP, the attacker creates a large number of half-opened TCP connections with a receiver or victim node, but never completes the handshake to fully open up the connection, this will lead to drain in energy. Another type of attack is session hijack, In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a Denial of Service (DoS) attack on the victim [6].

Thus the attacker impersonates the victim node and continues the session with the target. Hijacking a session over UDP is the same as over TCP, except that UDP attackers do not have to worry about the overhead of managing sequence numbers and other TCP mechanisms. Since UDP is connectionless, edging into a session without being detected is much easier than the TCP [6]. In our research we will focus on UDP and how to secure it using authentication mechanism and encryption technique.

0974-9756/CIIT-IJ-4000/05/$20/$100 © 2012 CiiT Published by the Coimbatore Institute of Information Technology

B. Application Layer attacks

The application layer communication is also vulnerable in terms of security compared with other layers. The application layer contains user data, and it normally supports many protocols such as HTTP, SMTP, RTP, and FTP [6], which provide many vulnerabilities and access points for attackers.

Malicious code attacks: Malicious code, such as viruses, worms, spywares, and Trojan Horses, can attack both operating systems and user applications.

These malicious programs usually can spread themselves through the network and cause the computer system and networks to slow down or even damaged. Repudiation attacks: Repudiation refers to a denial of participation in all or part of the communication [6].

These types of attacks can be defended by adapting asymmetric key system that is used for encryption. Our research will focus on the RTP protocol as it commonly used in data 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, most of them relied on providing security on physical layer, data link layer and network layer security for example in the military fields, Their goal was to limit the effect of node capturing, also known as node compromise by an attacker. Proposed countermeasures to node capturing included key management schemes are introduced in [7], [8] and location aware security [9]. Theses research didn't take to its consideration the energy metric. And other researches proposed energy schemes, e.g., [3] [10], have been proposed for creating an energy efficient mechanism for secure communication in the mentioned layers. In contrast, our research focuses on application and transport layer security with taking into consideration the energy metric.

The Mechanism proposed in this paper share some theoretical features with approaches in [3], but we grantee that our research is a unique one as the Network Simulator (NS-2) doesn't support any security features in all of its versions, but we succeeded to implement our secured mechanism on it.

Our research may be a base work to researchers to begin to use NS-2 as a security simulator. This research will help them 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 theses metrics in the following sections.

V. Proposed Mechanism

A. Design Assumptions

We assume a network consisting of 100 nodes. 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. Packet format modifications

We construct the secured packet format on the current packet format of communication across WSN [Figure 1].

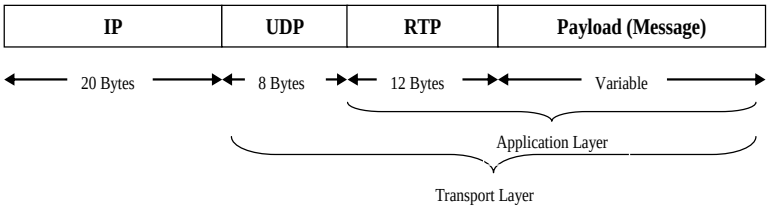

Fig. 1 Normal Packet Format

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

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

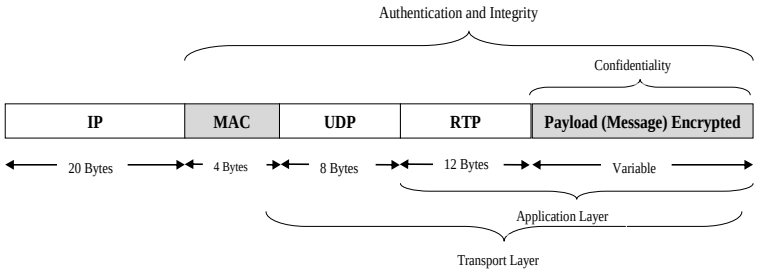

Fig. 2 Secured Packet Format

By applying the previous two mechanisms, we 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 [11].

C. Symmetric Encryption

The Advanced Encryption Standard (AES) [12] encryption was selected in our proposed mechanism 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 mechanism. The features of AES algorithm has been investigated and its effect on energy has been studied well in researches [12] [13]. 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 [14]. 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 [14] (CBC-MAC is secure only for fixed-length messages).

E. Implementation Details.

Ns-2 is an object-oriented simulator developed as part of the VINT project at the University of California in Berkeley [15]. 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. [15]

NS-2 can model essential network components, traffic models and applications. Typically, it can configure transport layer protocols, routing protocols, interface queues, and also data link layer mechanisms. We can easily see that NS-2 in fact could provide us a whole view of the network construction, meanwhile, it also maintain the flexibility for us to decide. Thus, just this one simulation tool can help us simulate nearly all parts of the network.

NS-2 doesn't support any security mechanism, but we succeed to build a core package to add security features in NS-2. From the NS-2 development view, [Figure 3] shows the layered architecture of NS-2.

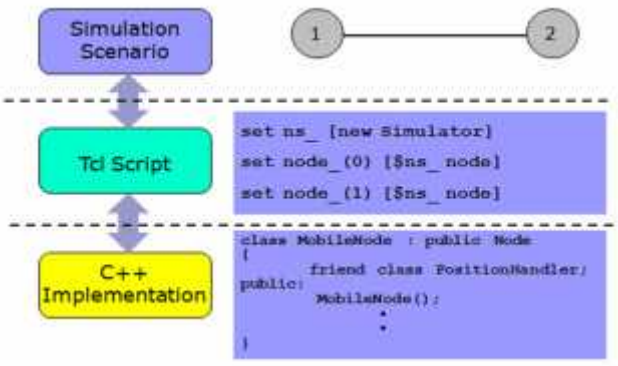

Fig. 3 Development layered view for NS-2

The lowest level of NS-2 is implemented by C++ which implements the event schedulers and most of the network components, and the Tcl script level is on top of it to make simulation stuffs much easier to be conducted. Then, upon the Tcl level, we see the overview of the network. That is the simulation scenario.

A security library (Crypto++) [16] is been added to C++ implementation layer. Crypto ++ is a free and open source C++ class library of cryptographic algorithms such as AES, DES, HMAC, CMAC..etc

The secured packet format is been implemented to adapt the changes as illustrated in [Figure 2] (application layer modification).

A new security protocol based on UPD protocol is been developed. The send and receive function is been changed to adapt the security features. The security features are AES encryption of the payload and the CMAC generation (transport layer modification).

The above changes in C++ implementation layer forced us to make changes in TCL Script. These changes enable us to use the new secured mechanism in simulation scenario. The main change is to create a TCL name for security mechanism (SECURITY_UDP).

[Figure 4] summarize all changes we developed in NS-2 codes to adapt our security mechanism.

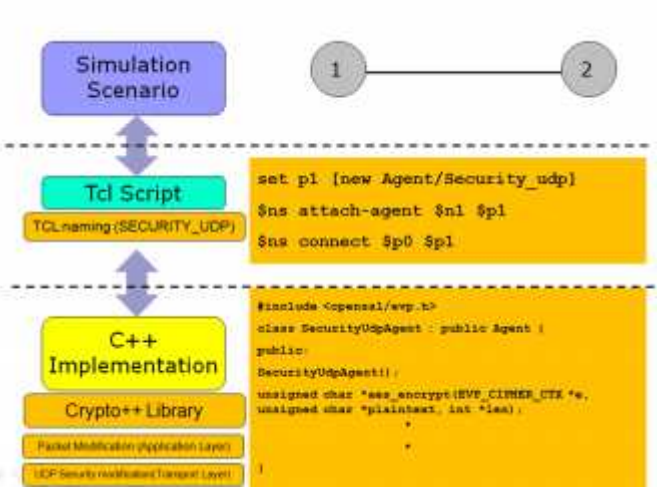

Fig. 4 Security Modifications for NS-2

To successfully carry out the proposed simulation scenario, NS-2 parameters must be set to adapt our security mechanism. So what we need is, set the following three necessary parameters:

1) Appearance of the network: the whole topology view of sensor network, this includes the position of nodes with (x, y, z) coordinate. We supposed that there is no movement in nodes.

2) Internal of the network: since the simulation is on the network traffic, it is important to configure (1) which nodes will be the sources, (2) how about the connections, and (3) what kind of secure connection will be used?

3) Configuration of the layered structure of each node in the network; this includes: (1) the detail configuration of network components on sensor node, (2) drive the simulation, (3) give out where to give out the simulation results which is the trace file, and (4) organize a simulation process.

The following section will illustrate the simulation parameters and how to assign them. Also demonstrates in

brief what are the metrics that will be measured especially the energy metrics.

VI. Simulations And Results

Before describing the three necessary parameters of the simulation scenario, a brief overview of the NS-2 simulation parameters is presented as shown in table II.

The first parameter is the network appearance. The network appearance was generated according to uniform distribution using MATLAB toolbox. [Figure 5] illustrates the position of nodes. We supposed that there is no movement in nodes.

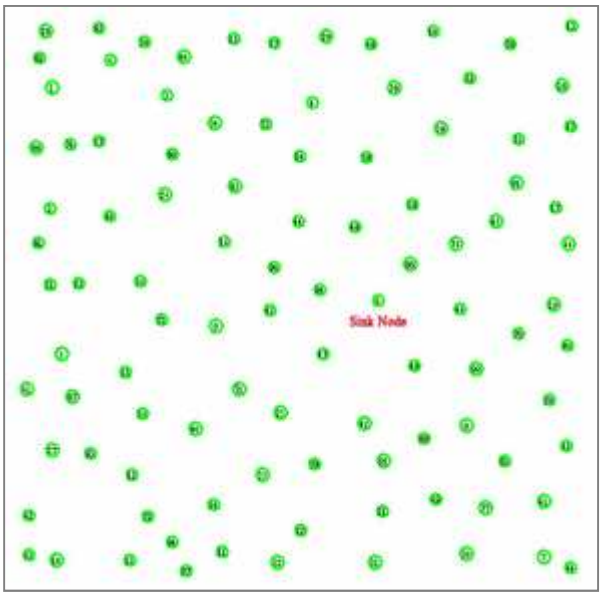

Fig. 5 The position of nodes in 1000M X 1000m Area

The second parameter is internal of the network. The internal of network means how to generate network traffic flow. We believe that most traffic is directed from the nodes to the sink node. The reason for that assumption is derived from the ultimate goal of a WSN; to get information from the network.

TABLE II
Simulation Parameters

Simulation Parameters	Values
Mac layer Protocol	IEEE 802.11 with prioritizing extension
Transmission Radio	250 M
Data Packet Size	Variable
Data Rate	2 packets/sec
Simulation Area	1000 M X 1000 M
Number of Sensor nodes	100
Node Initial Energy	100 J
Transmission Power	0.007
Reception Power	0.007
Simulation Time	120 sec

The third parameter is the configuration of layered structure of each node. The layered structure means which protocol to be used to send data payloads. Two types of protocol used in the proposed simulation; the UDP protocol which send data without any security (Naked UDP), and our proposed security mechanism (Secured UDP).

Our simulation results are presented in a trace file [Figure 6]. Trace file is a file generated by NS-2 simulations [12]. We used trace file to generate statistics about energy and others metrics.

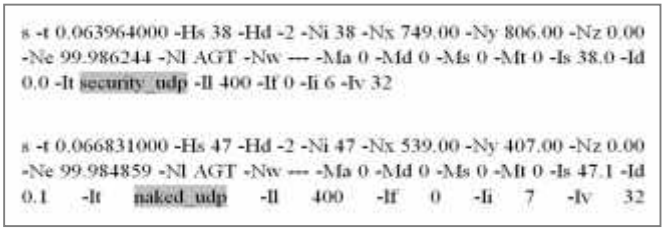

Fig. 6 Screen shot of a trace file generated by a simulation scenario

Our goal is to minimize energy as can as possible as data transmission takes 70 % of the total energy consumption of a wireless sensor network. The main idea is to reduce the number of secured data packets to be transmitted with a highest priority to reach to sink node first before any other data packets.

To achieve the previous goal, we modified the interface queue (IFQ) [15] to give our mechanism the highest priority beside the control packets which are already have the highest priority to be sent in the queue.

We reduce the number of transmitted secured packets by suggesting a hybrid secured network topology. The hybrid network topology depends on providing a security features only to sensor that contains a sensitive data to be protected.

The simulation scenarios are presented by securing 10%, 20%, 30%… 100% of the nodes in the network. During the simulation runs, another important parameter is found (The message length). Because we found a relation between the message length and the whole energy of network, we decided to add it to the simulation parameter.

Before displaying our results and analysis them, the energy of encryption process can be neglected when it measured with the data transmission. Many researchers studied this issue and found that in order to measure the energy for encryption process; the following encryption energy cost equation E_{enc} of for N_{PL} bits of plaintext can be used.

$$E_{enc} = (P_{cpu} * C_{enc} / f_{cpu}) * \lceil N_{PL} / u \rceil. \qquad (1)$$

Where P_{cpu} and f_{cpu} are the power and the frequency of the Sensor CPU respectively, and C_{enc} is the number of CPU cycles required to perform an encryption of a block of size u. The symbol $\lceil\ \rceil$ denotes the ceiling operator. According to research [17], the process of encryption consumed about 1 - 4 x 10^{-9} J per instruction cycle, which is small compared to energy used in transmission and reception which is 0.007 J. The energy consumption of encryption and decryption process

will not be included in simulation results.

The first measured metric is the packet delivery ratio of the secured mechanism which represented in [Figure 7]. The x axis represent a secured nodes varied from (10 – 100) nodes. The naked UDP which contains no security is represented by number 0 in x axis (zero secured nodes).

As mentioned before; simulation will be taken place in variable payload size and a message with 100 and 200 bytes is selected. When we increased the payload size to be more than 200 bytes; the network delivery ratio collapsed. The reason for that, the network can't handle the process of encryption and sending and receiving data packets at the same time. 100 bytes is enough to send payload data in a lot of application such as military application which sensors can send alerts and data message for example "tank seen in location X, Y".

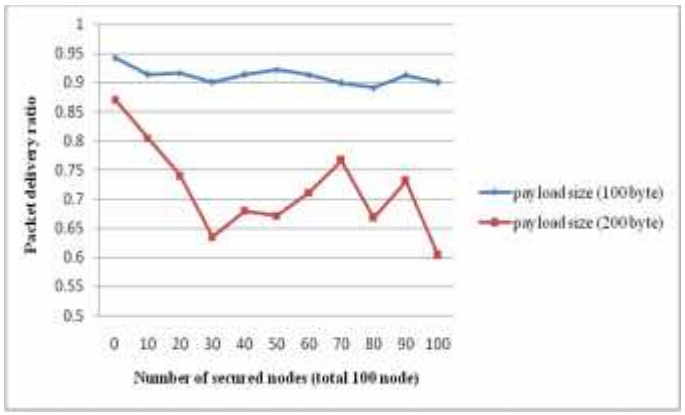

Fig. 7 the packet delivery ratio for hybrid security Topologies

Figure 7 illustrates that the secured mechanism for hybrid network (10 – 100 secured nodes) achieved a competitive packet delivery ratio from (0.9 to 0.93) with zero secured nodes which achieved (0.95) delivery ratio with message payload size 100 byte.

The second metric is the total energy consumption of the network under hybrid security topologies.

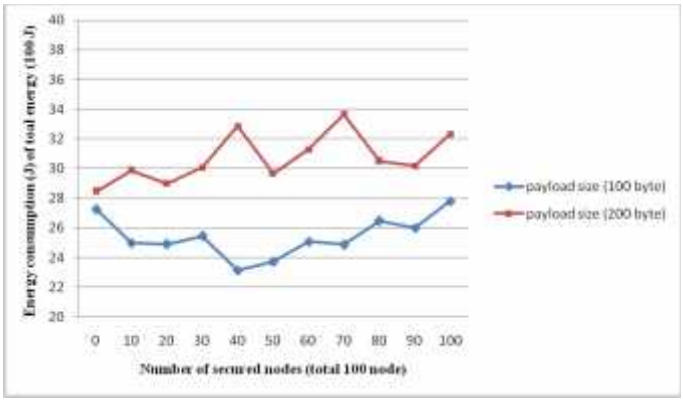

Fig. 8 The Total energy Consumption for hybrid security Topologies

Figure 8 illustrates that when payload size is 100 bytes it consumes less energy as it consume less energy in encryption and decryption process.

We are looking for the least energy consumption in the network and this has been achieved when 40% of network is secured, it consumes 23 % energy out from 100 % energy of the network during simulation time. It consumes 4 % less than zero secured nodes which consumed 27% energy of the network due to the IFQ priority list. IFQ gives a secured packet a highest priority rather than unsecured packets.

The third metric is the average energy consumption over packet delivery ratio. From figure 9, we can see clearly that the decision of choosing payload data size with 100 byte is the most suitable size for payload size for our security mechanism.

[Figure 9] also supports our decision of selecting a hybrid security network topology with 40 % of nodes to be secured which give the least energy consumption.

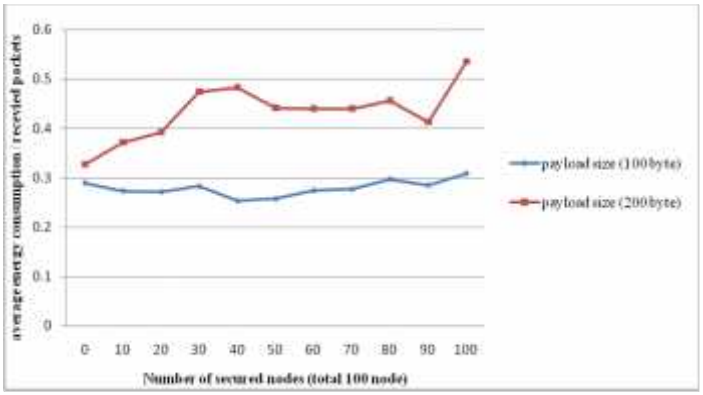

Fig. 9 The average Energy consumption / Received packet for Hybrid Security Topologies

According to our security goals mentioned in section II, we achieved all six goals. The goals are data authentication, Integrity, confidentiality, Freshness, Untethered energy consumption and network availability.

The last metric to be measured is the data overhead. The data overhead are mainly the increased size of RTP Packet for CMAC code which is 4 bytes. The network data will be over headed by to 11 % of its original data in case there is no security used in the network. The proposed mechanism will stand against all known attacks mention in section III which may be taken placed in the application and transport layer.

VII. Conclusions

This research has introduced a security mechanism for Wireless Sensor Networks. This research has shown that how the proposed mechanism has achieved the security goals and issues, and how it has operated. The proposed mechanism has been compared with other existing mechanisms that share common goals. Our security mechanism benefits from certain unique features and also builds on existing ideas currently present in the literature.

The proposed mechanism depends on securing the application and transport layer on AES encryption and CMAC message authentication. It is implemented using NS-2, according to our literatures reviews. This research can be

considered as the first research has succeeded to add security features in NS-2.

The RTP header and UDP protocol are modified to adapt the proposed security mechanism. A new idea for securing wireless sensor network is presented which lead to less energy consumption. The idea is to give a priority to the secured packet over the normal packet in IFQ. Also we deduced that securing only 40% of the network nodes leads to a significant improvement in network energy consumptions.

VIII. FUTURE WORKS

The presented security mechanism 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.

An improvement can be occurred also choosing other MAC codes and encryptions techniques; these can save significant amounts of wasted energy.

IX. REFERENCES

[1]. K. Kifayat, M. Merabti, Q. Shi and D. L. Jones," Security in Wireless Sensor Networks," Handbook of Information and Communication Security, Part E, pp. 513-552, 2010.

[2]. S. Ito and K. Yoshigoe, "Performance Evaluation of Consumed-Energy-Type-Aware Routing (CETAR) for Wireless Sensor Networks," International Journal of Wireless & Mobile Networks (IJWMN), Vol. 1, No. 2, pp. 93-104, 2009.

[3]. S. Sharma, "Energy-effcient Secure Routing in Wireless Sensor Networks," National Institute of Technology Rourkela, Msc Thesis, May 2009.

[4]. S. Mohammadi, R. E. Atani, and H. Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks," Journal of Information Security, Vol. 2, No. 2, pp. 69-84, April 2011.

[5]. M. Holland, T. Wang, B. Tavli, A. Seyedi, and W. Heinzelman, "Optimizing Physical Layer Parameters for Wireless Sensor Networks," ACM Trans. on Sensor Networks (TOSN), Vol. 7, No. 4, pp. 1-20, February 2011.

[6]. V.C Manju, "Study of security issues in wireless sensor network," International Journal of Engineering. Science and Technology (IJEST), Vol.3, No.10, pp. 7347- 7352, October 2011.

[7]. R. D. Pietro, L. V. Mancini, A. Mei, "Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks". Wireless Networks, Vol. 12, No. 6 ,pp. 709-721, December 2006

[8]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," Proc. of the ACM Conference on Computer and Communications Security, pp. 62–72, Washington, USA, October 2003.

[9]. H. Yang, F. Ye, Y. Yuan, S. Lu, and W. Arbaugh, "Toward Resilient Security in Wireless Sensor Networks," Proc. of the Sixth ACM international symposium on Mobile ad hoc networking and computing, pp. 34-45, Illinois, USA, May 2005.

[10]. F. Massicotte, F. Gagnon, Y. Labiche, L. Briand and M. Couture, "Automatic evaluation of intrusion detection systems," Proc. of the 22nd Annual Computer Security Applications Conference on Annual Computer Security Applications Conference, pp. 361– 370, Washington,USA,2006.

[11]. H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", RFC 3550, July 2003.

[12]. P.D. Khambre, S.S.Sambhare and P.S. Chavan, "Secure Data in Wireless Sensor Network via AES," International Journal of Computer Science and Information Technologies, Vol. 3, No. 2, March 2012.

[13]. S. Desai, S. Butani and S. Valiveti, "Analyzing the Impact of Standard Encryption Approaches for Data Aggregation in a Wireless Sensor Network," International Journal of Computer Science and Telecommunications, Vol. 3, No. 6, pp. 55-59, June 2012.

[14]. M. Dworkin, "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication," NIST Special Publication 800-38B, National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf; May 2005.

[15]. S. Siraj, A. Gupta and R. Badgujar, "Network Simulation Tools Survey," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, No. 4, pp. 199-206, June 2012.

[16]. W. Dai. Crypto++ library . http://www. cryptopp.com/, 2012.

[17]. N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," IEEE Transactions on Mobile Computing, Vol. 5, No. 2, pp. 128– 143, December 2005.

Nour El Din 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 in 2009. 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 H. Taha 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 Department of Information Technology, Faculty of Computers and Information, Cairo University in 2009. 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