International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 4 –AUGUST 2016.

Combating Energy Exploiting Assaults in Hierarchical Wireless Sensor Networks using IDEA

T R Shejin[#1] and Neethu Francis[*2]

[#]*PG Scholar, Department of Computer Science & Engineering, K.M.P College of Engineering, Odakkali, Kerala*

[*] *Assistant Professor, Department of Computer Science & Engineering, K.M.P College of Engineering ,Odakkali, Kerala*

***Abstract*— Safety measures and energy efficiency are the most significant concerns in wireless sensor networks (WSNs) design. To accumulate the power and enlarge the lifetime of WSNs, a range of media access control (MAC) protocols are proposed. Most conventional security solutions cannot be functional in the WSNs due to the constraint of power supply. The well-known safety measures mechanisms usually aware the sensor nodes before the sensor nodes can affect the security processes. However, the Denial-of-Sleep attacks can exhaustion the energy of sensor nodes and cut down the lifetime of WSNs rapidly. Therefore, the existing designs of MAC protocol are not enough to protect the WSNs from Denial-of-Sleep attack in MAC layer. The useful design is to make simpler the authenticating process in order to improve the performance of the MAC protocol in argue against the power exhausting attacks. This paper proposes a cross-layer design of secure scheme incorporate the MAC protocol with algorithm International Data Encryption Algorithm (IDEA) algorithm International Data Encryption Algorithm in order to make higher energy consumption and secure encryption. Assigning trust values to the nodes based on energy level. Interactions between nodes are performed by study of expectation value and multiple hops are selected according to, nodes having better energy objective functions value. The study shows that the proposed scheme can argue against the replay attack and forge attack in an energy-efficient way.**

Index Terms*— *wireless sensor networks, energy efficiency, denial of-sleep, power exhausting attacks, secure scheme, IDEA algorithm.

I. INTRODUCTION

Securing wireless sensor networks (WSNs) adds more challenges to the research. This is because WSN properties make it harder to be secured than other types of networks. In WSNs, applying a high security level imposes more resource and decreases the energy efficiency of network. Sensor networks are vulnerable to several malicious attacks. Since sensor batteries are severely limited, Denial of sleep attacks (DS attack) is recognized as one of the most serious threats. The DS attack [1] is a specific type of denial-of-service (DoS) attack that targets a battery powered device's power supply in an effort to exhaust this constrained resource and reduce the network life time.

Indeed, this attack tries to break in the device's power management system to reduce the opportunities to transition into lower power states. Since Mac layer is responsible for managing the radio transceiver, defensive strategies implemented at this layer are the most effective in protecting radio usage. S-MAC protocol [2] represents the baseline energy-efficient sensor MAC protocol designed to extend WSN network lifetime. In this medium access control protocol, sensor node periodically goes to the fixed listen/sleep cycle. A time frame in S-MAC is divided into two parts: one for a listening session and the other for a sleeping session. Only for a listen period, sensor nodes are able to communicate with other nodes and send some control packets such as SYNC, RTS (Request to Send), CTS (Clear to Send) and ACK (Acknowledgement). Using a SYNC packet exchange, all neighboring nodes can synchronize together. Radios in networks which use this protocol will be asleep at 90% of the time, thereby producing an almost tenfold improvement in node life.

A denial of sleep attacker can manipulate Mac protocol and cause nodes to expend additional energy. For example, an attacking node in a SMAC-based network could repeatedly send request-to-send messages (RTS) and force the node listed in the RTS destination field to respond with a clear-to-send (CTS) message and remain awake waiting for the follow-on message [3]. To provide a defense against this attack, most of existing researches propose authentication and encryption solutions or implement a complex and energy inefficient mechanisms. However, WSNs require simpler solutions to the same security challenges due to limited processing capability, memory storage, and energy capacity.

In the Low Power Listening (LPL) based WSN MAC convention, for example, In B-MAC, at the point when the sender needs to send information, it sends a long preamble to cover the sleep period to guarantee the receiver awakening and detecting. The LPL based MAC convention is a no concurrent convention, which decouples the sender and receiver with time synchronization. For example, the X-MAC convention is one of the sender initiated schema.

The X-MAC protocol develop LPL based MAC protocol by replacing the long preface with shot prelude. It shows the timeline of X-MAC protocol, which agree to the receiver to send acknowledgment (ACK) support to the sender as soon as it senses the prelude. The Denial of-Sleep is one of the power exhausting attacks of WSNs. This attack attempt to maintain

the sensor nodes awake to consume extra power. In any security method, the sensor nodes must be waked prior to receiving data and checking safety measures properties. Present layer-2 protocol designs are inadequate to protect a WSN from Denial-of-Sleep attack. Lacking security method, an anti-node can broadcast a false prelude frequently. If the receiver cannot inform the real preamble and the forged one, the receiver will receive and route the data from the anti-node. Such attack will keep the receiver wide awake as lengthy as the data transmission maintain, which exhausts the battery of nodes quickly. In addition, an anti-node can rerun a false preamble ACK to the sender. Thus, the sender will establish to send the data to the anti-node but it will in no way receive the correct data ACK. Similarly, the sender may send data frequently and exhausts the battery of node quickly. As a result, the sender and receiver need joint authentication schemes to argue against such attacks. In conventional wireless security system, the transmitting information is encrypted with keyed symmetric or asymmetric encryption algorithm.

The wireless sensor networks desire the symmetric algorithm to circumvent the complicated computing and heavy energy utilization. But the encrypted information makes the battery exhaustion still worse in Denial of- Sleep attack. The anti-node can launch the encrypted "junk" data to receiver. This attack armed forces the receiver to decrypt the information. Before the receiver recognizes that the data is "junk", the receiver use more power to receive and decrypt information. These methods also keep sensor nodes wide awake longer. An easy and quick mutual authentication scheme is needed to incorporate with MAC protocol to counter the encrypted "junk" data attack. In this paper The functional configuration is to improve the security process when enduring the force depleting attacks. The outline of security plan in upper layers might be combined with the settled information join layer system. In this paper, a cross layer configuration of secure plan incorporating the MAC convention, Two-Tier Energy-Efficient Secure Scheme (TE2S) with International Data Encryption Algorithm (IDEA), is proposed to shield the WSNs from the above attacks as well as to make the energy consumption using the energy objective functions in light of our preparatory systems

II. LITERATURE SURVEY

In this paper, we focuses on sleep deprivation attack which is also considered as layer 2 attack. This section gives an idea about the related mitigation technique of it.

The network lifetimes of existing Medium Access Control (MAC) protocols such as Sensor MAC (S-MAC), Timeout MAC (T-MAC) and Berkley MAC (B-MAC) were compared by Raymond et. al.[4]. Brownfield et. al. [5] had proposed a protocol Gateway MAC to mitigate the effects of denial of sleep attacks. WSNET link layer protocol G-MAC can serve as an effective denial of sleep defense by centralizing cluster management.

In [6], it is assumed that adversary nodes must become cluster heads in order to launch sleep deprivation attack. Three separate methods are analyzed for mitigating sleep deprivation attack: the random vote scheme, the round robin scheme, and the hash-based scheme.

In [7], have evaluated these schemes based upon their ability to reduce the adversary's attack, the amount of time required to select a cluster head and the amount of energy required to perform each scheme. It have been found that, hash-based scheme is the best among three clustering methods at mitigating the sleep deprivation attack in terms of resilience towards attack and required overhead.

In [8], a host based lightweight intrusion detection technique, Clustered Adaptive Rate Limiting (CARL) based on rate limiting approach at MAC layer is proposed to defeat denial-of-sleep attacks. In this adaptive rate limiting approach, network traffic is restricted only when sufficient malicious packets have been sensed to suspect that the network is under attack. It can be used to maintain network lifetimes and better throughput at a time even in the face of sleep deprivation attack.

In [9], a scheme is proposed employing fake schedule switch with RSSI measurement aid. The sensor nodes can reduce and weaken the harm from exhaustion attack and on the contrary make the attackers lose their energy quickly so as to die.

In [10], a quickest intrusion detection scheme, modeled as Markov Decision Process (MDP) has been proposed by keeping a minimal number of sensors active. Three sleep/wake scheduling algorithms are mentioned here. i) optimal control of the number of sensors in the wake state in a time slot. ii) optimal control of the probability of a sensor in the wake state in a time slot. iii) optimal probability of a sensor in the wake state. It ensures that energy expenditure for sensing, computation and communication is minimized and the lifetime of the network is maximized.

In [11]-[12], a dynamic session key policy (DSKP) was proposed based on a one time password (OTP) system to protect users during the authentication process and session key agreement process. The reason for using OTP is that it varies with sessions where the length is long enough compared with a human-chosen password [13]. Therefore, it is hard to trace and detect. By using the counter indicated hash-chain algorithm, the DSKP is computational cheap. But the synchronized counter of hash-chain algorithm may not be suited to the asynchronous LPL based MAC protocol in WSNs.

The overhead of security algorithms have been well studied on embedded systems [14]-[15]. Several popular algorithms of symmetric encryption and hashing function were evaluated on varied micro-controller units (MCU) in [15]. Based on experimental tests, the clock cycles and execution time were measured for each algorithm and platform. These analytical models can be derived to indicate the computational cost of given embedded architectures on different encryption schemes. However, the synchronized work against of hash-chain algorithm may not be suited to the asynchronous Low control Listening based MAC protocol in WSNs due to its complexity in keeping the work against synchronized in untrustworthy communication media.

The slide of security algorithms have been fit studied on embedded method. Several popular algorithms of symmetric encryption and hashing function were evaluated on varied

micro-controller component (MCU). Based on tentative tests, the timepiece cycles and execution time were measured for each algorithm and stage. These logical models can be derived to show the computational cost of the known embedded architectures on dissimilar encryption schemes. Inclusive surveys of design challenges and recently proposed MAC procedure, where the MAC protocols of WSNs are classifier and the classification of MAC protocols to help deciding a function.

III. EXISTING SYSTEM

The Existing Method, current layer-2 procedure designs are inadequate to maintain a WSN from Denial-of-Sleep attack. The power protection is one of the major goals of WSN plan, whereas the safety scheme forever consumes more power of method. There is no well choice rule to cooperation the supplies between power conservation and safety measures method. The Denial-of-Sleep is one of the power exhausting attacks of WSNs. This attack is an unusual type of Denial-of-Service (DoS) attack, which tries to wait the sensor nodes wide awake to use more power of the constrained power contribute. An anti-node can send false information packets to sensor node of vulnerable WSNs to initiate redundant transmissions frequently. Without security method, an anti-node can broadcast a false preamble commonly in the sender initiated schemes. If the receiver cannot inform the real prelude and the false one, the receiver will receive and method the data from the anti-node. Such attack will stay the receiver aware as long as the data broadcast sustains, which exhausts the sequence of nodes quickly.

IV. PROPOSED SYSTEM

This paper proposes a two-level secure transmission plan. This plan utilizes the hash chain to create the dynamic session key, which can be utilized for common confirmation and the symmetric encryption key. The main calculations of element session key are the hash capacities, for example, MD5 or SHA-1, which are extremely straightforward and quick. By coordinating with MAC convention, there is no additional bundle contrasted and the current MAC plans. The two-level outline can check and interfere with the attacks at various check points. The mix of low complexity security process and multiple check point can resistance against attacks and send the sensor node back to rest mode at the earliest opportunity. The security investigation demonstrates that this plan can counter the replay attack and forge attack, and for securing the system, we utilize the International Data Encryption Algorithm (IDEA), a sensor network service enabling effective network-wide energy decision making. IDEA is considered as one of the most important post-DES cryptographic algorithms, due to its high immunity to attacks, it is utilized for high throughput, guiding the network toward states that improve performance.

The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The fundamental innovation in the design of this algorithm is the use of operations from three different algebraic groups. The substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. The algorithm structure has been chosen such that, with the exception that different key sub-blocks are used, the encryption process is identical to the decryption process.

A. Advantages of the IDEA algorithm

This algorithm increase the cryptographic strength.

This algorithm reduce the weak keys problem in Daemon's report.

The accuracy of the predicted model should be good as compared to other existing algorithm.

This enhanced algorithm is increasing the security

B. SYSTEM ARCHITECTURE

The energy efficient architecture for power exhausting attacks is given in the figure 1.The basic goal of the proposed model is to reduce the energy that is exhausted from the node. This can be overcome by applying clustering method and key generation method to the node. This can be performed by detecting antinode to transmit the data. To detect the antinode the node wants to broadcast a hello message to the neighboring node.

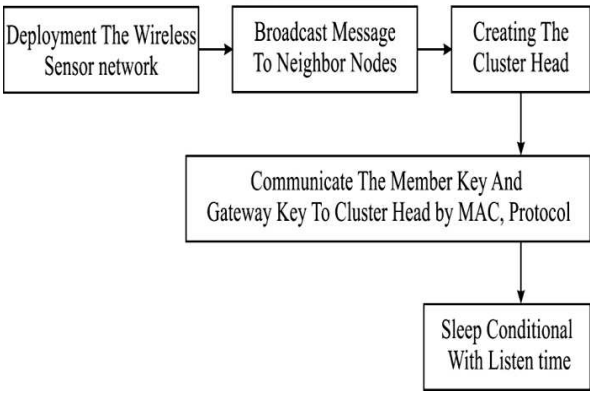

Fig.1 System Architecture

The neighboring node response with the correct key that is already provided means the neighboring node with the correct response form a cluster. If not means that one is mark as an anti-node and detected. And to select the cluster head the node which has a maximum response it is marked as a cluster head.

And then cluster gateway is selected thus the cluster member and the cluster head is selected. Then the key distribution phase is used to transmit the data at each node. The key is formed with the help of hash function. If the key is valid means the cluster member turn into a-wake state if not means it go back to the sleep state. Thus the power exhausting attack is considerably reduced. The source node broadcast the hello message to its neighbor nodes. The distributed key is passed to all sensor nodes. The nodes which are not able to decrypt the message will be the anti-node.

The nodes are grouped as the clusters. The cluster

formation is done by the received hello messages. The node which receives more acknowledged hello will be the cluster head and remaining are the cluster members. The communication between two cluster are done by the cluster gateway. Now the key is distributed within the cluster for data transmission process. Once the key is distributed the nodes access the data using the decryption process.

C. SYSTEM MODULES

1) Topology Formation

Wireless Sensor Nodes are deployed over a region where some phenomenon is to be monitored. Each node in the Wireless Sensor Network maintains the details of neighbor node.

2) Anti-Node Detection

In the authenticated broadcasting method, a plaintext "Hello" message is encrypted by the pre-distributed key as the broadcasting challenge. If the sensor cannot decrypt the received message effectively, the sender is said to be an antinode. Thus, the standard nodes and the anti-nodes can be making different.

3) Cluster Formation

When sensors are initial deployed, the ADTCA from may be used to separation the sensors into group.

a) Cluster head Selection:

Each sensor sets a random waiting control, broadcasts its occurrence via a "Hello" signal, and listens in for its neighbor's "Hello." The sensors that have the sense of hearing many neighbors are good quality candidates for initiating original clusters; those with little neighbors should wish to wait. Sensors revise their neighbor information (i.e., a counteract specifying how many neighbors it have detected) and reduce the random waiting time based on every "new" Hello message received. There are three special kinds of sensors: (1) the cluster heads (2) sensors among an assigned cluster ID (3) sensors without an assigned cluster ID, which will connect any close by cluster and turn into 2-hop sensors.

b) Gateway Selection:

To intersect two adjacent non-overlapping clusters, one cluster component from each cluster must turn into a gateway. According to the procedure of cluster configuration, sensors can get local information and identify the number of neighboring sensors in nearby clusters.

c) Key Distribution

In this stage, two symmetric public keys, a cluster key and a gateway key, are encrypted by the pre-distributed key and are distributed in the neighborhood. A cluster key is a key shared by a cluster head and its entire cluster component, which is mainly used for securing in the neighborhood broadcast messages, e.g., routing organize information, or securing sensor communication.

d) Key Renewal

Using the similar encryption key for extended periods may acquire a cryptanalysis threat. To keep the sensor network and avoid the adversary from getting the keys, key renewing may be required. Primarily all cluster heads (CHs) decide an inventor to start the "key regeneration", and then it will launch the index to all cluster heads in the set of connections.

e) Mutual Authentication

The dynamic session key Ks is a hash function and includes 3 items: Kc, Rs, and Rr. In these items, the Rs and Rr. are newly selected random numbers by the sender and receiver respectively. These random numbers will be changed every time to ensure the Ks to be created dynamically. The cluster key Kc is shared only by the valid member nodes of a cluster, which indicates that the sender and receiver are valid member nodes of cluster. Thus, the sender and receiver can be authenticated mutually.

f) Secure Token Replay Attack:

In Tier-1, an anti-node may replay the previous eavesdropped random number Rs and secure token h(Kc | Rs) as a fake preamble to the receiver. Since the random number Rs and secure token h(Kc | Rs) are created dynamically during the transmission session, they are different in every session. The receiver can record and ignore the recent Rs and h (Kc | Rs) to resist the repeatedly secure token replay attack. Note that the number of recorded recent Rs and h (Kc | Rs) may depend on the memory amount of sensor nodes.

g) Forge Attack:

Without known Kc, an anti-node cannot compute the new dynamic session key Ks. It is infeasible to compute the h(Ks) from h(h(Ks)) nor to compute the Ks from h(Ks).

(1) Fake Preamble ACK Attack:

In Tier-1, an anti-node may send a fake preamble ACK to deceive the sender to keep sending data and therefore consuming energy. Since the receiver must compute h(h(Ks)) from Ks, the valid h(h(Ks)) can be used to protect the sender against fake preamble ACK attack from anti-node.

(2) "Garbage" Data Attack:

In Tier-2, an anti-node may send "garbage" data to cheat the receiver to go into the step of decrypting data and therefore consuming energy. Since the sender cannot compute the h(Ks) from received h(h(Ks)), the valid h(Ks) can protect the sender against "garbage" data attack from an anti-node.

D. IDEA Algorithm

The proposed method using IDEA algorithm, with an existing routing protocol. In the first encryption round, the first four 16-bit key sub-blocks are combined with two of the 16-bit plaintext blocks using addition modulo 216, and with the other two plaintext blocks using multiplication modulo 216 + 1. The results are then processed further as shown in Figure 1, whereby two more 16-bit key sub-blocks enter the calculation and the third algebraic group operator, the bit-by-bit exclusive OR, is used. At the end of the first encryption round four 16-bit values are produced which are used as input to the second encryption round in a partially changed order. The process described above for round one is repeated in each of the subsequent 7 encryption rounds using

different 16-bit key sub-blocks for each combination. During the subsequent output transformation, the four 16-bit values produced at the end of the 8th encryption round are combined with the last four of the 52 key sub-blocks using addition modulo 216 and multiplication modulo 216 + 1 to form the resulting four 16-bit cipher text blocks.

An IDEA (International Data Encryption Algorithm) is a universally applicable block encryption algorithm, which permits the effective protection of transmitted and stored data against unauthorized access by third parties in wireless sensor network.

V. PERFORMANCE EVALUATION

A. *Simulation Parameters*

The NS2 tool [16] is used to study the performance of our proposed method. We employ the IEEE 802.11 [17] MAC with a channel data rate of 11 Mb/s . We choose the two evaluation metrics: number of nodes transmitted from source to destination, number of nodes performed in the MAC layer and the average number of bits send in the node for a packet to be transmitted from the source to destination using IDEA.

TABLE I. STIMULATION PARAMETERS

Parameter	Value
Application Traffic	10 CBR
Transmission rate	4 packets/s
Packet Size	512 bytes
Channel data rate	11 Mbps
Area	700m*700m
Simulation time	800
Duration of node sleep (TS)	500
Duration of node awake (TW)	25
Duration of preamble transmitting (Tp)	2
Duration of preamble ACK listening (TPAL)	20
Duration of preamble ACK (TPA)	2
Maximum duration of preamble transmitting	500
Duration of data transmitting (TD)	4
Duration of data ACK transmitting (TDA)	2
Duration of idle listening before sleep	20

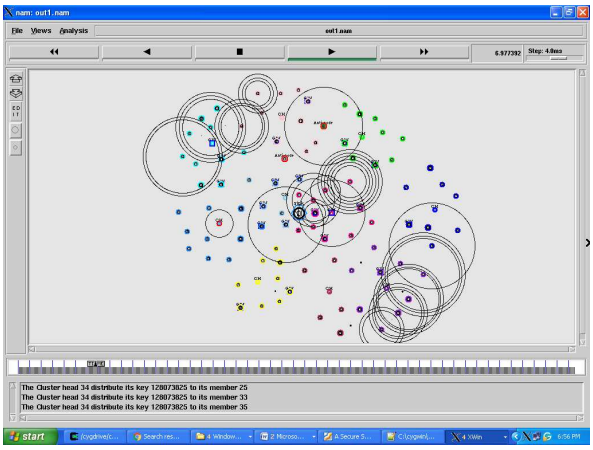

Fig.2 Network Topology with IDEA algorithm

B. *Simulation Results*

We used the performance metrics to validate the proposed algorithm with results obtained in this papers are shown in Figure 3,4 and 5.

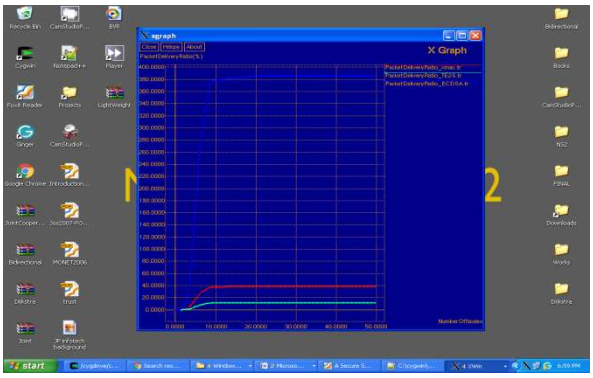

Fig.3 Packet delivery ratio

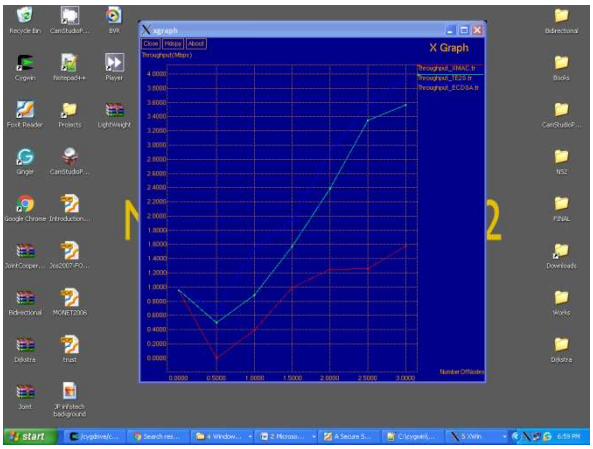

Fig. 4 Throughput

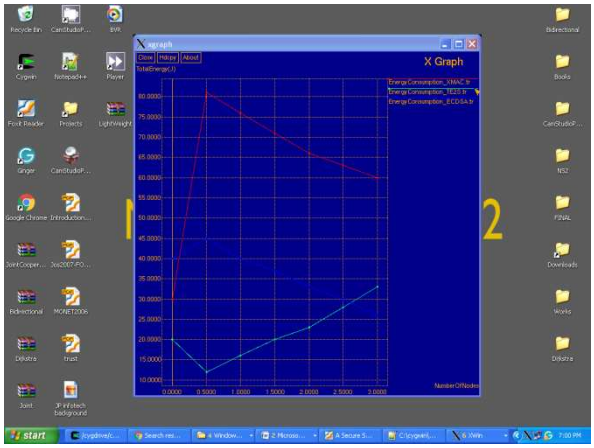

Fig. 4 Energy consumption

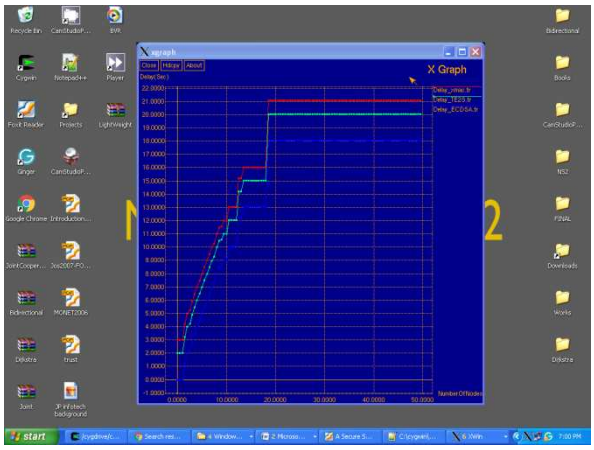

Fig.5 Delay

Thus the proposed scheme is very significant and effective when comparing with existing methods.

VI. CONCLUSION

This paper proposes a cross-layer plan of energy-efficient protected system integrating the International Data Encryption Algorithm (IDEA), a sensor network service enabling effective network-wide energy decision making. No additional packet is involved in the new proposed procedure design. This method can reduce the authenticating procedure as short as probable to mitigate the result of the power exhausting attacks. The safety measures analysis shows that this scheme can contradict the replay attack and forge attack as provide the energy consumption using IDEA algorithm with effective energy objective function in the wireless sensor network. The power analysis identifies the operating method accurately, including the MCU and radio modules. The model result of normalized power consumption shows that the proposed scheme increases 4.08% in power consumption, below the packet sending time of 1 small package every 3 seconds. The energy investigation shows that this system is well-organized. Further power consumption of the proposed system under various information packet rate and attack situation will be investigated in the expectations. More LPL based WSNs MAC protocols additional than X-MAC, such as B-MAC, will be adopted to grant more widespread simulation results to maintain the effectiveness of TE2S With IDEA algorithm. The assessment will also expand from single node to multiple nodes.

REFERENCES

[1] R. C. Carrano, D. Passos, L. C. S. Magalhaes, and C. V. N. Albuquerque, “Survey and taxonomy of duty cycling mechanisms in wireless sensor networks,” IEEE Commun. Surv Tuts, vol. 16, no. 1, pp. 181–194, First Quarter 2014.
[2] M. Li, Z. Li, and A. V. Vasilakos, “A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues,” Proc. IEEE, vol. 101, no. 12, pp. 2538–2557, Dec. 2013.
[3] J. Kabara and M. Calle, “MAC protocols used by wireless sensor networks and a general method of performance evaluation ,” Int. J. Distrib. Sensor Netw, vol. 2012, pp. 1–11, 2012, Art. ID 834784.
[4] A. Bachir, M. Dohler, T. Watteyne, and K.K. Leung, “MAC essentials for wireless sensor networks,” IEEE Communications Surveys & Tutorials, vol.12, no.2, pp. 222-248, second Quarter 2010.
[5] D. Raymond, R. Marchany, M. Brownfield and S. Midkiff, “Effects of denial of sleep attacks on wireless sensor network MAC protocols, ”IEEE Transactions on Vehicular Technology, vol. 58, no. 1, Jan. 2009.
[6] R. Falk, and H.J. Hof, “Fighting insomnia: a secure wake-up scheme for wireless sensor networks,” in Proc. SECURWARE, Athens, 2009, pp. 191-196.
[7] Y. C. Ouyang, C. T. Hsueh, and H. W. Chen, “Secure authentication policy with evidential signature scheme for WLAN,” Security and Communication Networks, vol. 2, no. 3, May/June 2009, pp. 259-270.
[8] Y. C. Ouyang, C. B. Jang, and H. T. Chen, “A secure authentication policy for UMTS and WLAN inter working,” in Proc. IEEE ICC, Glasgow, 2007, pp. 1552-1557.
[9] M. Buettner, G. V. Yee, E. Anderson and R. Han, “X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks,” in Proc. ACM SenSys, Boulder, 2006, pp. 307-320.
[10] M. Brownfield, Y. Gupta, and N. Davis, “Wireless sensor network denial of sleep attack,” in Proc. 6th Annu. IEEE SMCIAW, 2005, pp.356-364.
[11] G. P. Halkes, T. V. Dam, and K. Langendoen, “Comparing energy saving mac protocols for wireless sensor networks,” ACM Mobile Networks and Applications, vol. 10, no. 5, pp. 783-791, Oct. 2005.
[12] J. Polastre, J. Hill, and D. Culler, “Versatile low power media access for wireless sensor networks,” in Proc. ACM SenSys, Baltimore, 2004, pp. 95-107.
[13] T. van Dam and K. Langendoen, “An adaptive energy-efficient mac protocol for wireless sensor networks,” in Proc. ACM SenSys, Los Angeles, 2003, pp. 171-180.
[14] Y. C. Ouyang, R. L. Chang, and J. H. Chiu, “A new security key exchange channel for 802.11 WLANs,” in Proc. IEEE ICCST, Taipei, 2003, pp. 216-221.
[15] W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient mac protocol for wireless sensor networks,” in Proc. INFOCOM, New York, 2002, pp. 1567- 1576.