ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

IMPROVING NETWORK LIFETIME IN HIERARCHICAL WIRELESS SENSOR NETWORKS USING SECURITY AWARE MECHANISMS

R. SriRohini[1], S. Ramesh [2]
[1]Pg Scholar, Anna University Regional Campus, Madurai, India
[2]Professor/CSE, Anna University Regional Campus, Madurai, India
rohini.srirohini@gmail.com, rameshcse@autmdu.ac.in

Abstract- Wireless sensor network is one of the prominent technology that provides a wide range of applications. It provides a way for several different applications like military application, industrial application and health monitoring application. Energy and security are the major factor that affect the lifetime of the network. Mac layer protocol must be energy efficient to maximize the network lifetime. Mac protocol are inadequate to protect the nodes from different types of possible attacks like jamming attack , garbage attack, denial of sleep attack. To encounter the power exhausting attacks in Mac protocol this paper proposes the cross layer design of secure scheme desegregating the Mac protocol. To solve security problem it proposes a two tier secure transmission scheme. This scheme uses a hash chain to generate dynamic session key for mutual authentication and symmetric encryption key and Two Tier energy efficient secure key management for improving network lifetime. For performance analysis, conduct a NS 2 simulation and investigate that the scheme can increase the reliability, packet delivery ratio and packet loss.

Keywords—MAC protocol , Network Lifetime, Mutual Authentication ,DOS Attack, power exhausting , Jamming attack .

I. INTRODUCTION

Wireless sensor network is one of the promising technology that provide wide range of application .It combines sensing ,computation and communication into a single device. It is mainly designed for real-time analysis of data in hostile environment. It has hundreds to thousands of nodes in a network and connected to form a network. Energy is a major factor that affect the lifetime of the network. It can be extended using various schemes. Energy conservation of wsn can be done using duty-cycle based protocol. The sensor nodes are switched among active and sleep state occasionally and are switched into sleep mode after certain idle period. These approaches are designed for energy saving: one at the mac layer (S-MAC and T-MAC)and other at Low Power Listening .Low power listening(LPL) protocols are an asynchronous protocol such as B-MAC , X-MAC and RI-MAC and it helps to reduce idle listening by replacing the long preamble. S-MAC protocol is a sensor mitigates idle listening. It is a contention based protocol where time is divided into large time frames. It uses virtual clustering in which nodes send synchronized message. It achieves good scalability and collision avoidance. In T-MAC protocol which adapts the duty cycle to network traffic. It uses timeout period to determine the end of an active period.

In B-MAC protocol the receiver awake occasionally to intellect the preamble from the sender and then data is processed by receiver. When the sender wants to transmit data, it transmits a long preamble to hide the sleep period to make certain that the receiver is waking up and sensing. Sender and receiver decouples mutually for time synchronization. It is classified into two types: sender-initiated scheme and receiver initiated scheme. The X-MAC protocol is a sender-initiated scheme and improves LPL by exchanging the long preamble by short preambles which permits the receiver to transmit ACK assist to the sender immediately it senses the preamble. The RI-MAC protocol is the receiver initiated schemes to reduce the channel occupancy time which permits the sender to send acknowledgment (ACK) assist to the receiver immediately it senses the beacon.

Denial of Service (DoS) attacks is still unanswered attacks on wireless sensor networks. DoS attack on a WSN is also called as sleep deprivation attack. This try to keep the sensor node awake to consume more energy of the power supply. An invader prevents a sensor node from going to a sleep state by constantly interacting with the sensor node, e.g. by constantly sending data requests. In sender initiated scheme the antinode transmits wake data packets to sender to start unnecessary transmission. It sends fake preamble frequently in this scheme. The receiver cannot find the real preamble and fake one. Hence it receives and process the data. It interns keeps receiver awake and exhaust the battery of the node. In receiver initiated scheme , the antinodes transmits the fake beacon to cheat sender and it process and send the data to antinodes. It will never receive the right ack. The receiver will start to receive and process the data from the antinode. The communication between the nodes in wsn could be interfered by attack packets. jamming like scenario is caused no packets can be delivered from the attacked nodes, This degrade the performance of the duty cycle scheme and energy conservation of antinode can be attained during an attack. Replay attack takes a part of message and plays them again to same or different receiver. Encryption algorithm is not sufficient to counter against the attack.

It either uses keyed symmetric or asymmetric algorithm. The WSN favor symmetric algorithm to prevent energy consumption and computing. Layer 2 is insufficient to fight against attack so cross layer design is used. The protocols of different layer are independent. It involves connecting two layers at design time without new interface for information sharing.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

For security purpose, the sensor node must be awake before receiving security process. In this scheme the upper layer must be combined with data link layer. Two-Tier Energy –Efficient Secure key management protocol is used to protect the WSN from the above attacks. It is done by integrating the MAC protocol. The major features of this scheme are energy consumption, low complexity, mutual authentication, and symmetric encryption, and dynamic session key, counters against denial of sleep attack. It uses hash chain to create dynamic session key for symmetric encryption and mutual authentication.MD5 and SHA-1 are the hash chain for creating dynamic session key and they are simple and fast. The design can ensure and disrupt the attack at different check points. It sends the sensor node back to snooze as early as possible.

The rest of this project is organized as follows: Chapter 2 explains the related work of the project. Chapter 3 discusses the system architecture. Chapter 4 explains the design principles of Two tier energy efficient secure key management. Chapter 5 provides the simulation results of the Two tier energy efficient secure key management. Chapter 6 concludes the project with future work.

II. RELATED WORK

Low power listening protocol the receiver occasionally turns on the radio and detect preamble and continue receiving until the symbol arrives. If there is no preamble the radio turned off.

In B-MAC protocol is a low power listening based protocol [19], here both the sender and receiver are used for time synchronization. The receiver is wake up occasionally and senses the preamble from the sender and the process the data

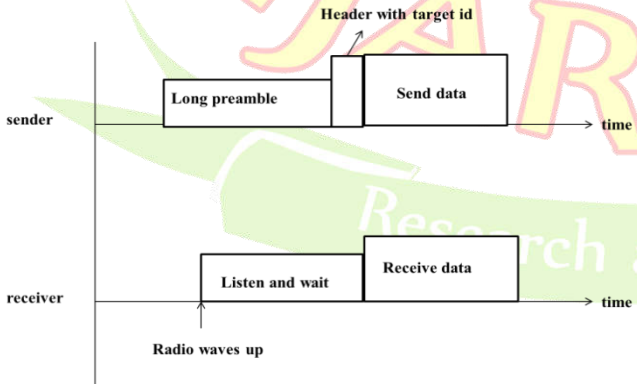

Figure 1 Timeline of B-MAC Protocol

. When sender needs to send data it sends long preamble to cover the sleep period to make sure that the receiver is awaken. ACK is not involved in B-MAC protocol. Receiver has to listen and wait for the long preamble from the sender. It utilize major energy and inadequate to protect against the attack. X-MAC protocol [1] is a sender initiated scheme improves B-MAC protocol by replacing long preamble with short preamble. A main goal is to achieve low latency, high throughput for data. It also focus on non-target receivers and make them to go back to sleep. The short preamble packets include address of the target receivers. It sends ACK back as soon as it sends the long preamble it also reduce energy consumption of both the sender and receiver.

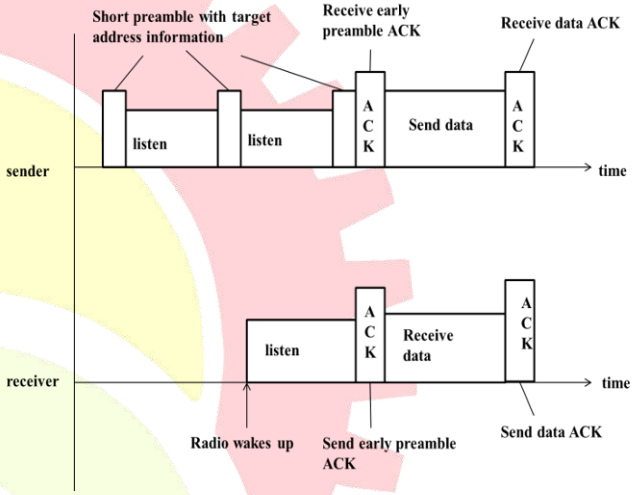

Figure 2 Timeline of X-MAC Protocol

RI-MAC is a receiver initiated scheme [17]. Receiver initiated data transmission protocol the receiver occasionally turns Low power listening protocol the receiver occasionally effectively operate traffic loads. It not only reduces overhearing but also achieves collision probability and recovery cost is less. Data frame is transmitted to initiate the transmission. RI-MAC achieves the packet delivery ratio and latency to sustain power efficiency. It allows the sender to send ack and data back to receiver as soon as it senses the beacon.

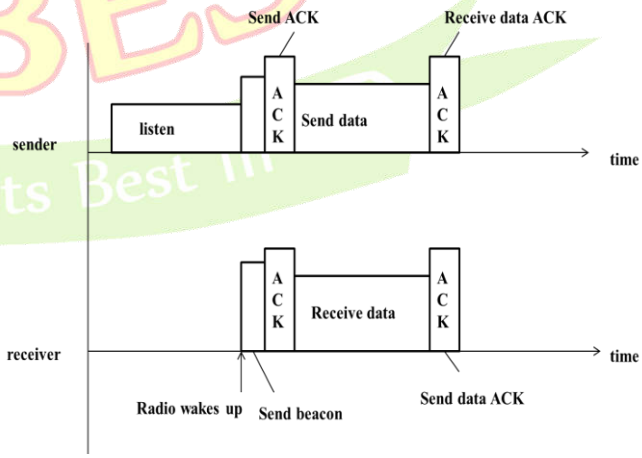

Figure 3 Timeline of RI-MAC Protocol

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

In [13], Authenticating process is done by means of session key agreement process uses dynamic session key policy (DSKP) with one time password to protect the system. When the password length is large compared with human chosen password is the reason use OPT. It is hard to trace and detect and they are computationally cheap. DSKP policy is not suited for asynchronous LPL based MAC protocol.

Synchronous LPL based MAC protocol [12] uses symmetric encryption and hashing function were evaluated on micro controller unit. Based on results, execution time and clock cycles are measured for each algorithm.

In [4], a Distributed and key management protocol is designed to satisfy authentication and confidentiality. The protocol is used for message broadcast each share its pair wise key with neighbors. It is based on hop-by-hop encryption, allowing nodes to share keys. The protocol offer security against a huge number of attacks. It ensures that data steadily arrive to the base station.

III. SYSTEM ARCHITECTURE

The main goal of the model is to reduce the energy that is drained from the node. This can be overcome by applying clustering method and key generation method to the node. Secure adaptive topology control algorithm is involved to confirm hierarchical topology. 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. The topology is formed by means of four phases and they are antinode detection, cluster formation, key distribution and key renewal.

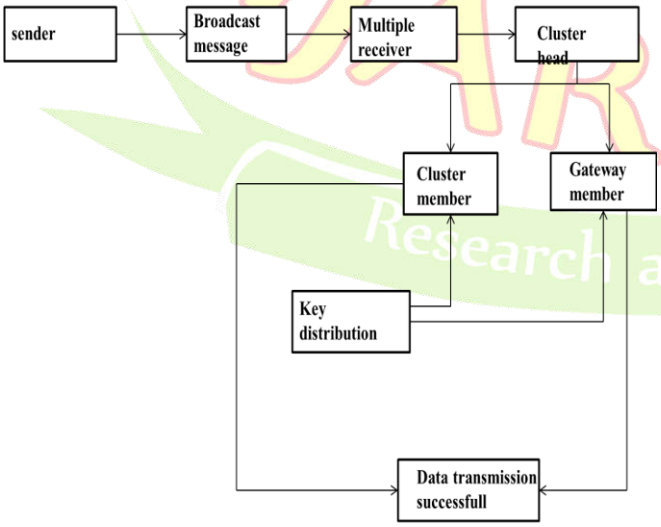

Figure 4 System architecture of energy efficient scheme

For an antinode detection it uses authenticated broadcasting mechanism to make network robust against attack .Denial of sleep attack is one of power exhausting attack and tries to keep sensor node awake to consume energy. Antinode sends fake data packets i.e. a plain text hello message to sensor node for unnecessary transmission. The plain text is encrypted by means of pre distributed key. If the sensor node cannot decrypt the message then the node is said to be antinode. The network without antinode is safe.

The sensors are deployed, ADTCA algorithm are used to partition the sensor into clusters. The cluster formation is done by means of clusterhead selection and gateway selection. It broadcast “hello” signals and listen for the neighboring hello. It initiate new cluster and neighbors with many neighbors become cluster head. To interconnect two adjacent non-overlapping clusters, one cluster member from each cluster must become a gateway and it broadcast message for connectivity information.

Symmetric key, cluster key and gateway key are distributed locally. Cluster key is used between cluster head and cluster member for locally broadcasting message. To protect the sensor network and prevent the opponent from getting the keys, key renewing may be necessary. The pre distributed key is ignored after the cluster key and gateway key is created. There is an establishment of inter cluster and intra cluster communication is made between cluster key and gateway key. At the start cluster heads want an inventor to start the "key renewals”, and it sends the index to every cluster heads.

The total energy is calculated using the formula

Consumed energy =initial energy – final energy

Initial energy is used at the starting point of the process and final energy is the energy produced at the final stage

IV. DESIGN PRINCIPLES OF T2ESKM

The proposed cross-layer design, Two-Tier Energy Efficient Secure key management is used to protect the WSN from the denial of sleep attack. It is done by integrating the MAC protocol. This scheme involves coupling upper layer with data link layer for information sharing. It uses hash chain to create dynamic session key for symmetric encryption and mutual authentication. It takes place in three steps and they are sender initiated scheme, data transmission and receiver initiated scheme. It has a pre distributed key and a pair wise key. The pre distributed key is used in memory of a sensor node before they are deployed. It is recycled for a limited period. In pair wise key one key is used among the cluster head and cluster members and the other is used between cluster head and base station. B-MAC protocol is not appropriate to incorporate mutual authentication. The basic architecture has been designed with X-MAC and RI-MAC protocol.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

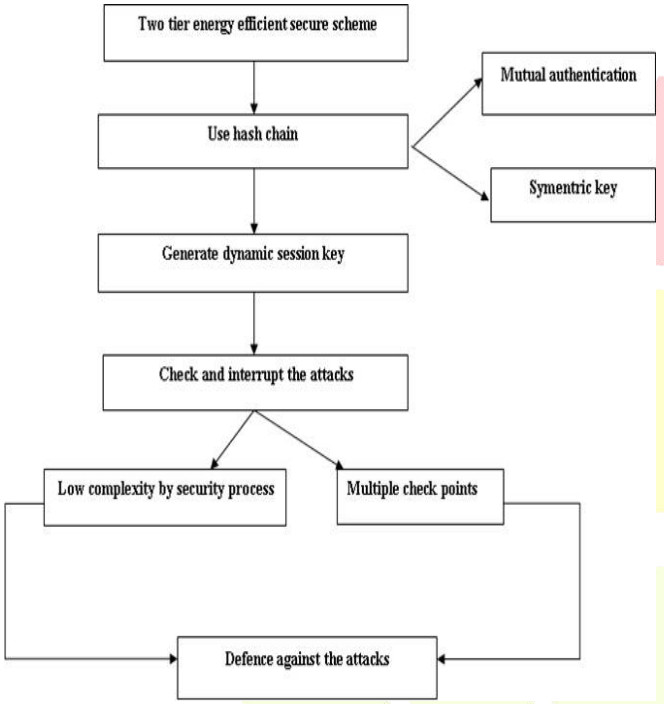

Figure 5 Design principles of T2SKM

In pair wise key one key is used among the cluster head and cluster members and the other is used between cluster head and base station. B-MAC protocol is not appropriate to incorporate mutual authentication. The basic architecture has been designed with X-MAC and RI-MAC protocol.A Keyed one time hash chain is created using cluster key C_k and it is shared among cluster head and cluster member.

A. Sender initiated scheme

Step 1: The random number is selected by the sender S_r. computes a secure token. (Token=$h(C_k|S_r)$

Step 2:It sends sender id, receiver id ,random number as preamble.

Step 3: The token is been verified by the receiver. If it is valid the receiver selects the random number and compute the key and hash chain ($S_k=h(C_k|S_r|R_r)$). If it is not valid go to sleep instantly.

Step 4: ($h(S_k)$ and $h(h(S_k))$ is verified and if it is not valid then sender will not send data

B. Receiver initiated scheme

Step 1: The random number is selected by the receiver R_r. computes a secure token.(Token=$h(C_k|S_r)$

Step 2:It sends sender id, receiver id ,random number as beacon by receiver.

Step 3: The token is been verified by the sender. If it is valid the receiver selects the random number and compute the key and hash chain ($S_k=h(C_k|R_r|S_r)$). If it is not valid go to sleep instantly.

Step 4: ($h(S_k)$ and $h(h(S_k))$ is verified and if it is not valid then receiver will not send data.

Either sender or receiver can initiate the communication. It depends by the design of the scheme. To check the token is legal it practices one hash chain and a one computing. It reaches dynamic session key agreement which select one random number selection and three hash functions.

C. Data Transmission

Dynamic session key (S_k) is created , the sender encrypts the data via symmetric encryption.

Step 1: The sender sends hash function ($h(S_k)$) an Mac(data) to the receiver.

Step 2: If $h(S_k)$ is verified by the receiver. If it is valid it decrypts the data and MAC of data is checked. If it is not valid it goes to sleep.

Step 3: The ACK is send by the receiver to the sender.

V. IMPLEMENTATION

The proposed scheme is evaluated through NS2 simulator. We consider a random network of sensor nodes and they are deployed in 1000 X 1000 area with a fixed base station. The type of antenna direction is Omni direction and the data type is link layer. To evaluate the performance the metrics are energy consumption, packet delivery ratio, throughput, latency and overhead.

A. Energy consumption

We compare the proposed protocol with T2ESKM to determine energy consumption. We measure it using the key update. Energy consumption of sensor node follows different network size. By experiment it is found that the number of node increases from 50 to 250 and the attackers varies from 10 to 20. It is the energy consumption and the attack interval. It is compared with T2ESKM and MAC protocols with it are a packets sending rate of 1 packet

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

every 3 seconds. We can notify that the gap between the two protocol extremely low and practically identical.

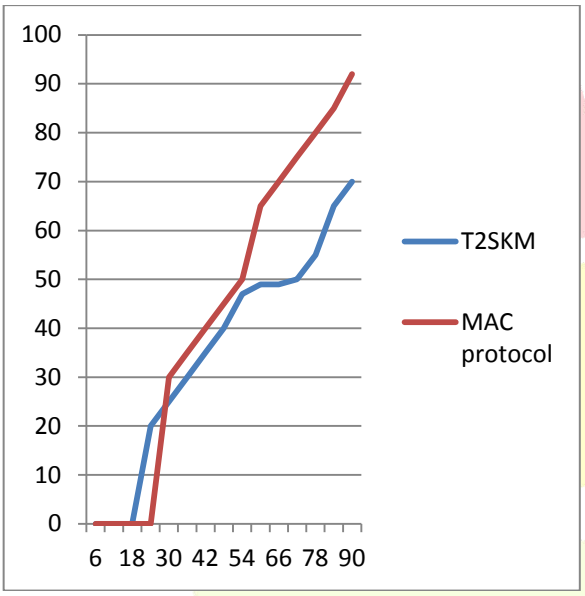

Figure 6 Comparison of Energy consumption in T2ESKM with existing MAC Protocol

This figure shows the analysis results energy consumption of each nodes. Here X-axis represents the time period values in second and y-axis represents the values in data bits

B. Packet delivery ratio

It is defined as the ratio of number of data packets received over the number of data packets sent. T2ESKM protocol has higher packet delivery ratio than Mac protocol.

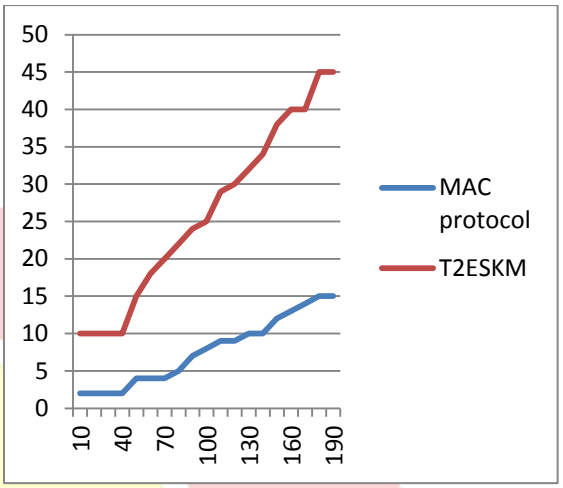

Figure 7 Comparison of packet delivery ration inT2ESKM with existing MAC protocol

C. Throughput

The packet is defined as the number of packets received and transmitted successfully. Using T2ESKM protocol there is an improvement in throughput and prevents the attack and it is shown in graph.

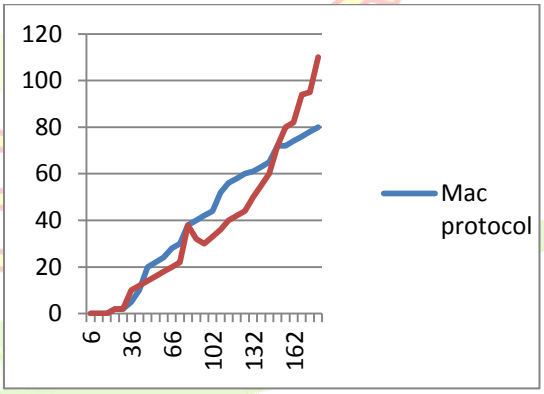

Figure 8 Comparison of throughput in T2ESKM with existing MAC Protocol

VI. CONCLUSION

In this paper, we proposed a two tier Energy Efficient Secure Key Management Scheme (T2ESKMS). This design process is used to reduce energy consumption.

Through performance evaluation, we discover the overhead, which the T2ESKMS protocol leads to is satisfactory level, and decrease the memory overhead. The Energy consumption is reduced using this protocol and also the lifetime of the nodes is raised.

Simulation results and analysis shows that our approach is more beneficial in energy efficient and storage than other schemes .Our future is to improve the security protocol by incorporating trust establishment and its management in sensors.

REFERENCES

[1] Buettner M.,Yee G.V.,Anderson E., and Han R.(2006), 'X-MAC: a short preamble MAC protocol for duty-*cycled wireless sensor networks,' in Proc. ACM SenSys* : Proceedings of the 4th International Conference on Embedded Networked Sensor Systems, Boulder, USA, pp.307-320.

[2] Carrano R. , Passos D., Magalhaes L., and Albuquerque C.(2013), 'Survey and Taxonomy of Duty Cycling Mechanisms in Wireless Sensor Networks,' IEEE Communications Surveys & Tutorials, No. 99, pp. 1-14.

[3] Falk R., and Hof H.J.(2009), 'Fighting insomnia: a secure wake-up scheme for wireless sensor networks,' in Proc. SECURWARE : Proceedings of the 3rd International Conference on Emerging Security Information, Systems and Technologies, Glyfada, Athens, 2009, pp. 191-196.

[4] Ganesan .P, Venugopalan. R, Peddabachagari .P, Dean .A, Mueller .F, and Sichitiu .M, "*Analyzing and modeling encryption overhead for sensor network nodes,*" in Proc. ACM WSNA':,San Diego, USA, 2003, pp. 151-159.

[5] Halkes G.P., Dam T.V., and Langendoen K.(2005), *"Comparing energy-saving MAC protocols for wireless sensor networks*," ACM Mobile Networks and Applications, Vol. 10, No. 5, pp. 783-791.

[6] Hsueh C.T., Li Y.W., Wen C.Y., and Ouyang Y.C.(2010), '*Secure adaptive topology control for wireless ad-hoc sensor networks*", sensors, Vol. 10, No. 2, pp. 1251-1278.

[7] Hsueh C.T.,Wen C.Y., and Ouyang Y.C.(2012), 'Two-tier receiver-initiated secure scheme for hierarchical wireless sensor networks, 'in ITST: Proceedings of the 12th International Conference on ITS Telecommunications, Taipei, Taiwan, pp. 254-258.

[8] Hsueh C.T., Wen C.Y., and Ouyang Y.C.(2015), 'A Secure Scheme For Power Exhausting Attacks In Hierarchical Wireless Sensor Networks,' IEEE Sensor Journal,Vol. 26,No. 6.

[9] Huang P., Xiao L., Soltani S., Mutka M.W., and Xi N.(2013), 'The Evolution of MAC Protocols in Wireless Sensor Networks: A Survey,' IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, pp. 101-120.

[10] Kabara J., and Calle M.(2012), 'MAC protocols used by wireless sensor networks and a general method of performance evaluation,' International Journal of Distributed Sensor Networks, Vol. 20, Article ID 834784, 11 pages.

[11] Li M., Li Z., and Vasilakos A.V.(2013), 'A survey on topology control in wireless sensor networks: taxonomy, comparative study, and open issues,' Proceedings of the IEEE, Vol. 101, No. 12, pp. 2538-2557.

[12] Liu .W, Luo .R, and Yang .H(2009), "Cryptography overhead evaluation and analysis for wireless sensor networks," in Proceedings of the International Conference on Communications and Mobile Computing, Kunming, China, 2009, pp. 496-501.

[13] Ouyang Y.C.,Hsueh C.T., and Chen H.W.(2009), 'Secure authentication policy with evidential signature scheme for WLAN,' Security and Communication Networks, Vol. 2, No. 3, pp. 259-270.

[14] Perrig .A, Szewczyk .R, Tygar J.D., Wen V., and Culler D.E.(2002), "SPINS: security protocols for sensor networks," Wireless Networks, 2002, Vol. 8,No. 5, pp. 521-534.

[15] Polastre .J, Hill .J, and Culler .D(2004), "Versatile low power media access for wireless sensor networks," in Proc. ACM SenSys Baltimore, USA, 2004, pp. 95-107.

[16] Raymond .D,Marchany .R, Brownfield .M, and Midkiff .S(2009), "Effects of denial of sleep attacks on wireless sensor network MAC protocols," IEEE Transactions on Vehicular Technology, Vol. 58, No. 1, pp.367-380.

[17] Sun .Y, Gurewitz .O, and Johnson .B.D(2008), "RI-MAC: a receiver-initiated asynchronous duty cycle MAC protocol for dynamic traffic loads in wireless sensor networks," In Proc. *ACM* Proceedings of the 6th International Conference on Embedded Networked Sensor Systems, Raleigh, USA, pp. 1-14.

[18] Van Dam T., and Langendoen k.(2003), "An adaptive energy-efficient MAC protocol for wireless sensor networks," Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, pp. 171-180.

[19] Ye .W, Heidemann .J, and Estrin.D(2002), "An energy-efficient MAC protocol for wireless sensor networks," in Proc. INFOCOM, pp. 1567-1576.