International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 3 Issue 6, May 2016

ISSN: 2394-4404

Two-Tier Energy Efficient Secure Scheme Against Power Exhausting Attacks In WSN's

Lakshmi M B

M.Tech (DCN),
Department of Telecommunication Engineering,
Dr.AIT, Bangalore

Chandrakala V

Associate Professor,
Department of Telecommunication Engineering,
Dr.AIT, Bangalore

Abstract: ***Wireless sensor networks have become an active research area. The sensor nodes are generally unattended after this deployment in hazardous, hostile or remote areas. These nodes have to work with their limited and non replenishable energy resources, hence energy efficiency is one of the main design objectives for the sensor networks. Although various Media Access Control(MAC) protocols have been proposed to save the power and extend the life time of WSN's ,the existing designs are insufficient to protect sensor networks from denial of sleep attacks. This paper aims to develop two-tier energy efficient secure scheme(TE2S) to protect WSN's from power exhausting attacks. This cross layer design involves coupling two layers at design time without creating new interface for information sharing at runtime. Energy conservation of WSN can be done using duty-cycle based proposed protocol.***

Keywords: wireless sensor networks, secure scheme, energy efficiency.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have emerged as one of the dominant technology trends of this decade that has potential usage in defence and scientific applications[1]. These WSNs can be used for different purposes such as target tracking, intrusion detection, wildlife habitat monitoring, climate control and disaster management. A typical node in the WSN consists of a sensor, embedded processor, moderate amount of memory and transmitter/receiver circuitry. These sensor nodes are normally battery powered and they coordinate among themselves to perform a common task[2].

These Wireless Sensor Networks have severe resource constrains and energy conservation is very essential. The sensor node's radio in the WSNs consumes a significant amount of energy. Substantial research has been done on the design of low power electronic devices in order to reduce energy consumption of these sensor nodes. Because of hardware limitations further energy efficiency can be achieved through the design of energy efficient communication protocols. Medium access control (MAC) is an important technique that ensures the successful operation of the network[3]. One of the main functions of the MAC protocol is to avoid collisions from interfering nodes. The classical IEEE 802.11 MAC protocol for wireless local area network wastes a lot of energy because of idle listening. Designing power efficient MAC protocol is one of the ways to prolong the life time of the network[4].

The Denial-of-Sleep is one of the power exhausting attacks of WSNs. This attack is a special type of Denial-of-Service (DoS) attack, which tries to keep the sensor nodes awake to consume more energy of the constrained power supply. The LPL based MAC protocol is an asynchronous protocol[5], which decouples the sender and receiver with time synchronization.

This long preamble design of LPL based protocol consumes the major energy of both sender and receiver. For instance, the X-MAC protocol is one of the sender-initiated schemes to improve B-MAC protocol by replacing the long preamble with short preambles, which allows the receiver to send acknowledgment (ACK) back to the sender as soon as it senses the preamble. The RI-MAC protocol is one of the receiver-initiated schemes to minimize the channel occupancy time of a pair of a sender and receiver[7] , which allows the

sender to send data to the receiver as soon as it senses the beacon. In this paper, a cross layer design of secure scheme integrating the MAC protocol[8], Two-Tier Energy-Efficient Secure Scheme (TE2S), is proposed to protect the WSNs from the above attacks based on our preliminary frameworks.

II. RELATED WORK

The Berkeley Media Access Control (B-MAC) is a contention based MAC protocol for WSNs. B-MAC is similar to Aloha with Preamble Sampling, which duty cycles the radio transceiver i.e. the sensor node t1urns ON/OFF repeatedly without missing the data packets. However in B-MAC, the preamble length is provided as parameter to the upper layer. computation and large payload of data that can be embedded in cover image with high visual quality. B-MAC, a carrier sense media access protocol for wireless sensor networks that provides a flexible interface to obtain ultra low power operation, effective collision avoidance, and high channel utilization[9]. To achieve low power operation, B-MAC employs an adaptive preamble sampling scheme to reduce duty cycle and minimize idle listening. B-MAC supports on-the-fly reconfiguration and provides bidirectional interfaces for system services to optimize performance, whether it be for throughput, latency, or power conservation. We build an analytical model of a class of sensor network applications[10].

III. PROPOSED METHOD

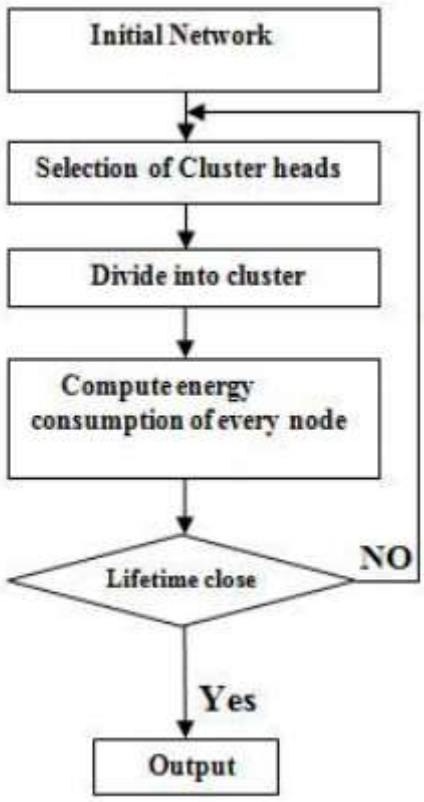

Figure 1: Flow chart of the proposed system

In any adopted security mechanism of WSNs, the sensor nodes must be waked before receiving data and checking security properties. The practical design is to simplify the security process when suffering the power exhausting attacks. The design of security scheme in upper layers may be coupled with the fixed data link layer mechanism. This paper proposes a two-tier secure transmission scheme.

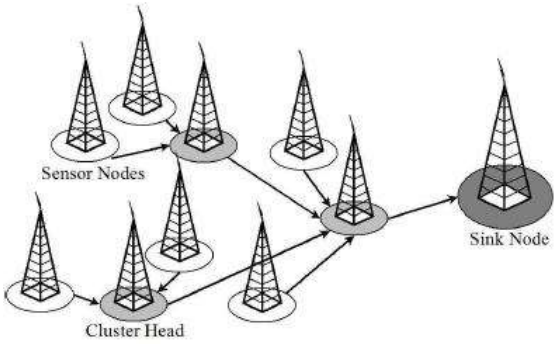

Figure 2: Cluster based sensor network model

This scheme uses the hash-chain to generate the dynamic session key, which can be used for mutual authentication and the symmetric encryption key. The only computations of dynamic session key are the hash functions, such as which are very simple and fast. By integrating with MAC protocol, there is no extra packet compared with the existing MAC designs. The two-tier design can check and interrupt the attacks at different check points. The combination of low complexity security process and multiple check points design can defense against attacks and send the sensor nodes back to sleep mode as soon as possible. The security analysis shows that this scheme can counter the replay attack and forge attack, and the energy analysis shows that this scheme i is energy efficient as well. The detailed energy distribution of energy analysis also shows a new possible decision rule to compromise the needs between energy conservation and security scheme.

Since the LPL based B-MAC protocol has no ACK mechanism, it is not suitable to integrate mutual authentication security mechanism without modifying the original B-MAC protocol design. In this work, the X-MAC and RI-MAC protocols are involved as the basic architectures of the proposed security scheme[11].

Figure 3: key distribution between the clusters

A. TIER-1: SESSION KEY AGREEMENT

In Tier-1, a hash-chain is created by using the cluster key Kc, which is the shared secret between the valid members and the cluster head. Depending on the different initiator, the duty-

cycle scheme can be classified into two types: sender-initiated scheme and receiver initiated (RI) scheme. This hash-chain is used for mutual authentication and symmetric encryption key[12].

ENCRYPTION ALGORITHM

✓ *SENDER-INITIATED SCHEME*

STEP 1: The sender selects a random number Rs and computes the secure token (i.e. *Token* = *h*(Kc|Rs), where *h*(x) denotes a one-way hash function with input x, and the vertical bar | denotes concatenation of strings)[13].

STEP 2: The sender sends its ID (IDs), receiver's ID (IDr), secure token and random number Rs as the preamble.

STEP 3: The receiver verifies the secure token. If the token is not valid, the receiver goes back to sleep mode immediately. If the token is valid, then receiver selects a random number Rr and computes the session key Ks = *h*(Kc|Rs|Rr). The receiver also computes the hash chain *h*(Ks) and *h*(*h*(Ks)).

STEP 4: The receiver sends the *h*(*h*(Ks)) and random number Rr as the ACK.

STEP 5: The sender computes the session key Ks = *h*(Kc|Rs|Rr) and the hash chain *h*(Ks) and *h*(*h*(Ks)). The sender then verifies the *h*(*h*(Ks)). If the *h*(*h*(Ks)) is not valid, the sender will not send the data.

✓ *RECEIVER-INITIATED SCHEME*

STEP 1: The receiver selects a random number Rr and computes the secure token (i.e. *Token* = *h*(Kc| Rr), where *h*(x) denotes a one-way hash function with input x, and the vertical bar | denotes concatenation of strings).

STEP 2: The receiver sends its ID, sender's ID, secure token and random number Rr as the beacon.

STEP 3: The sender verifies the secure token. If the token is not valid, the sender neglects the beacon and goes to beacon listen mode. If the token is valid, then sender selects a random number Rs and computes the session key Ks = *h*(Kc|Rs|Rr). The sender also computes the hash chain *h*(Ks) and *h*(*h*(Ks)).

B. TIER-2: DATA TRANSMISSION

With the new created dynamic session key Ks, the sender can encrypt the transmission data via symmetric encryption.

ENCRYPTION ALGORITHM

STEP 1: The sender sends the *h*(Ks) and EKs(DATA |MACKs(DATA)) to receiver. The EKs(x) denotes encrypts x by using symmetric algorithm with key Ks. The MACKs(DATA) denotes the message authentication function with key Ks, where DATA is the input message.

STEP 2: The receiver verifies the *h*(Ks). If the *h*(Ks) is not valid, the receiver goes back to sleep mode immediately. If the *h*(Ks) is valid, the receiver decrypts the data and checks the MAC of data.

STEP 3: The receiver sends the data ACK to sender.

IV. EXPERIMENTAL RESULTS

The algorithm is coded in NS-2 simulations on the energy consumptions of proposed TE_2S and run on a Windows 7 platform. In this simulation, the hashing function, and the encryption/decryption Algorithm is used because they are computational cheap and suitable for sensor network. We assume the number of nodes to be 32 in this simulation. These nodes are divided into clusters and cluster head is chosen for each cluster[14]. Session key generation and data transmission are the two methods followed in TE_2S scheme. Session key generation deals with selecting a random number and computing secure token. The random number selection is simplified as the hashed output of node ID and timer. Based on these assumptions, the individual energy consumption of security operations is evaluated[15].

ENERGY DEPLETION FOR TRANSMISSION

Depletion = unit of data × unit of distance × energy needed for transmission per bits

ENERGY DEPLETION FOR RECEPTION

Depletion = unit of data × unit of distance × energy needed for reception per bits

ENERGY DEPLETION FOR IDLE MODE

Depletion = unit of time × energy needed for idle mode

TOTAL ENERGY DEPLETION

TED = Depletion of transmission + depletion of reception + depletion of idle node

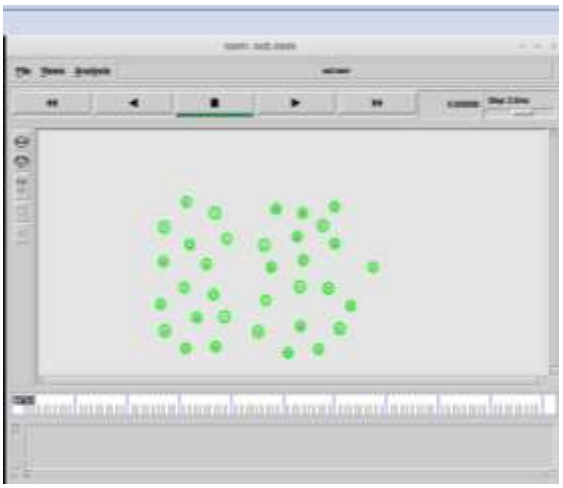

Figure 4: Creation of nodes

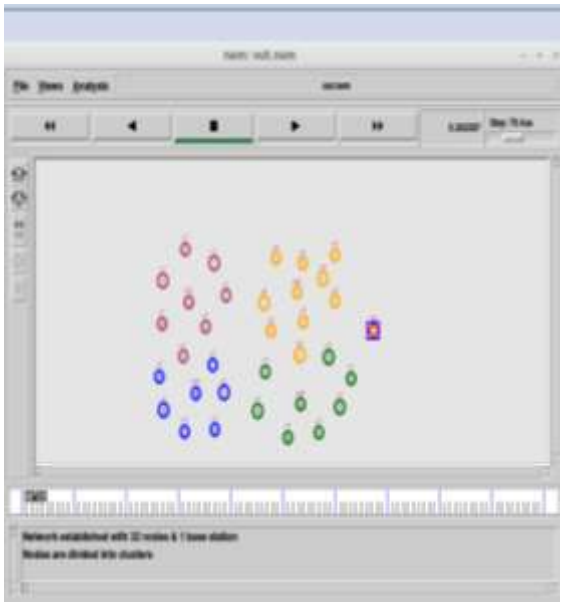

Figure 5: Cluster formation

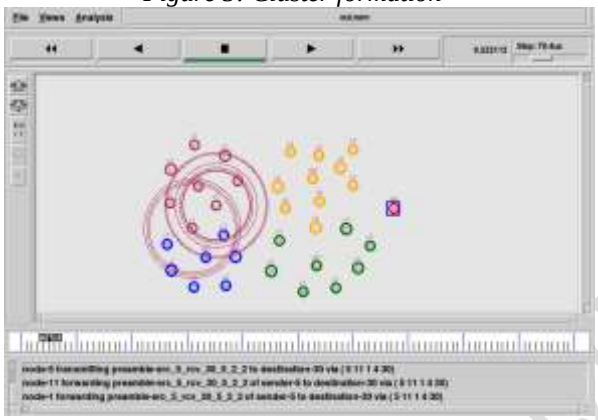

Figure 6: Transmitting data

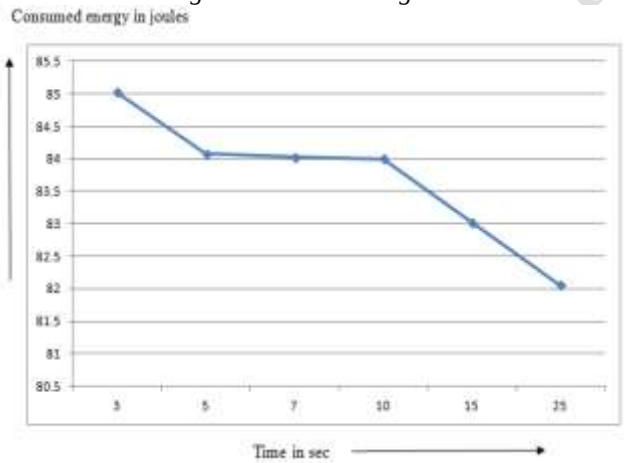

Figure 7: Energy consumption

SL no	Name of the Author	Time (sec)	Energy consumption
1	Ching-Tsung Hsueh and Chih-Yu Wen	3	88.15
2	Vasaki ponnusamy	5	88.08
		7	88.07
		10	97.02
3	Proposed system	15	96.08
		25	96.09
		25	**82.02**

Table 1: Energy analysis

V. CONCLUSION AND FUTURE WORK

This paper proposes a cross-layer design of energy-efficient secure scheme integrating the MAC protocol. No extra packet is involved in the original MAC protocol design. This scheme can reduce the authenticating process as short as possible to mitigate the effect of the power exhausting attacks. By combination of low complexity security process and multiple check points, the proposed design can defense against attacks and send the sensor nodes back to sleep mode as soon as possible. The security analysis shows that this scheme can counter the replay attack and forge attack. Future work is to improve security analysis by incorporating per-hop security process to avoid black hole attacks.

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 Commun. Surv. Tuts.*, vol. 12, no. 2, pp. 222–248, Second Quarter 2010.

[5] G. P. Halkes, T. van Dam, and K. G. Langendoen, "Comparing energy saving MAC protocols for wireless sensor networks," *Mobile Netw. Appl.*, vol. 10, no. 5, pp. 783–791, 2005.

[6] 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.

[7] Hsueh C. T., Li Y. W., Wen C. Y., and Ouyang Y.., '*Secure adaptive topology control for wireless ad-hoc sensor networks*", sensors, Vol. 10, 2010, No. 2, pp. 1251-1278.
[8] Hsueh C. T., Wen C. Y., and Ouyang Y. C, 'Two-tier receiverinitiated secure scheme for hierarchical wireless sensor networks, 'in ITST: Proceedings of the 12th International Conference on ITS Telecommunications, Taipei, Taiwan,2012, pp. 254-258.
[9] Hsueh C. T., Wen C.Y., and Ouyang Y.C, 'A Secure Scheme For Power Exhausting Attacks In Hierarchical Wireless Sensor Networks,' IEEE Sensor Journal,Vol. 26,2015,No. 6.
[10] Huang P., Xiao L., Soltani S., Mutka M.W., and Xi N, 'The Evolution of MAC Protocols in Wireless Sensor Networks: A Survey,' IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, pp. 101-120,2013.
[11] Kabara J., and Calle M., '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, 2012, 11 pages.
[12] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "Two-tier receiver-initiated secure scheme for hierarchical wireless sensor networks," in *Proc. 12th Int. Conf. ITS Telecommun. (ITST)*, Taipei, Taiwan, 2012, pp. 254–258.
[13] Y.-C. Ouyang, R.-L. Chang, and J.-H. Chiu, "A new security key exchange channel for 802.11 WLANs," in *Proc. IEEE 37th Annu. Int. Carnahan Conf. Security Technol. (ICCST)*, Taipei, Taiwan, Oct. 2003, pp. 216–225.
[14] Halkes G.P., Dam T. V., and Langendoen K, *"Comparing energysaving MAC protocols for wireless sensor networks*," ACM Mobile Networks and Applications, Vol. 10, No. 5, 2005, pp. 783-791.
[15] Van Dam T., and Langendoen k, "An adaptive energy-efficient MAC protocol for wireless sensor networks," Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, 2003,pp. 171-180.