ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Energy-Efficient Secure Key Distribution System In Hierarchical Wireless Sensor Networks

S.Manikandan, V. Nagaraj, B. Prabakaran, R. Sathiskumar

Assistant Professor, Dept. of ECE, VSA Group of Institutions, Salem, Tamilnadu, India

Assistant Professor, Dept. of ECE, VSA Group of Institutions, Salem, Tamilnadu, India

Assistant Professor, Dept. of ECE, VSA Group of Institutions, Salem, Tamilnadu, India

Assistant Professor, Dept. of ECE, VSA Group of Institutions, Salem, Tamilnadu, India

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. 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 trust value. The study shows that the proposed scheme can argue against the replay attack and forge attack in an energy-efficient way.

KEYWORDS: wireless sensor networks, energy efficiency, denial of-sleep, power exhausting attacks, secure scheme.

I.INTRODUCTION

To keep energy and enlarge the lifetime of WSNs, different schemes are researched and proposed. Most of the researchers plan at layer-2 protocol design. In the duty-cycle based WSNs MAC protocols, the sensor nodes are control between awake/active and sleep position from time to time. The sensor nodes are control into sleep mode after assured idle period. In the Low control Listening based WSNs MAC protocol, such as B-MAC, the receiver awaken up from time to time to sense the preface from the sender and then to receive and process the data. When the sender needs to send data, it sends a long preface to cover the sleep phase to ensure the receiver awaken up and sensing. The LPL based MAC protocol is an asynchronous set of rules. It decouples the sender and receiver with time management. 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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

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, a cross-layer design of secure system integrating the MAC protocol, Two-Tier Energy-Efficient Secure system (TE S), is proposed to keep the WSNs from the on top of attacks. The practical aim is to make simpler the security method when suffering the power exhausting attacks.

II.RELATED WORKS

The B-MAC is a Low control Listening based WSN MAC procedure, which decouples the sender and receiver with time management. The receiver wakes up from time to time to sense the prelude from the sender and after that to receive and route the data. When the sender wants to send information, it sends an extensive preamble to cover the sleep stage to guarantee the receiver waken up and sensing. It proves the timeline of B-MAC procedure. The B-MAC procedure has no ACKs and the receiver has to listen in and to stay for the long prelude ended from the sender. This lengthy preamble design of LPL based procedure consumes the main power of both sender and receiver. The X-MAC procedure improves LPL based B-MAC protocol by replacing the extensive preamble with little preambles. It proves the timeline of X-MAC procedure, which allocate the receiver to send ACK support to the sender as soon as it senses the prelude. These short prelude designs reduce the power consumption of equally the sender and receiver. The RI-MAC procedure reduces the channel tenancy time of a matchup of a sender and receiver. It proves the timeline of RI-MAC procedure, which permit the sender to send acknowledgment (ACK) and data reverse to the receiver as soon as it senses the signal. In an active session key policy (DSKP) was proposed based on a one time password (OTP) scheme to keep users during the verification method and session key conformity process. The basis for using OTP is that it varies with gathering where the time taken is long a sufficient amount compared with a human-chosen secret word. Therefore, it is tough to trace and detect. By using argue against indicated hash-chain algorithm, the DSKP is computationally low-cost. 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

III.EXISTING METHOD

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 METHOD

This paper aims to develop an energy-efficient secure method against power exhausting attacks, particularly the denial-of-sleep attacks, which can cut down the lifetime of WSNs quickly. Although different media access control (MAC) procedure have been proposed to keep the power and expand the lifetime of WSNs, the existing plan of MAC protocol are inadequate to keep the WSNs from denial-of-sleep attacks in MAC layer. This is attributed to the detail that the well-known safety measures mechanisms usually wide awake the sensor nodes earlier than these nodes are allowed to execute the safety measures processes. In any adopted security method of WSNs, the sensor nodes must be waked before receiving information and checking safety measures properties. The practical aim is to make simpler the security process when suffering the influence exhausting attacks. The design of safety measures scheme in upper layers may be coupled with the fixed data link layer system.

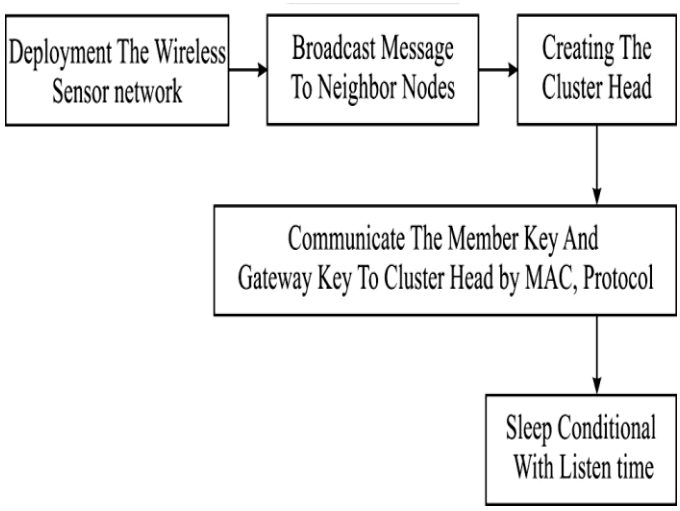

Figure1.1 Proposed Flow Diagram

In this paper, a cross- layer aim of secure method integrating the MAC procedure, Two-Tier Energy-Efficient Secure Scheme (TE2 S), is proposed to protect the WSNs from the above attacks based on our beginning frameworks. This

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

cross-layer plan involves coupling two layers at aim time without creating new boundary for in sequence sharing at runtime.

V.MODULE DESCRIPTION

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.

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 anti-node. Thus, the standard nodes and the anti-nodes can be making different.

Cluster Formation

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

1) 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.

2) 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.

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.

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

VI.SECURITY ANALYSIS

A. Mutual Authentication

The dynamic session key K_S is a hash function and includes 3 items: K_C, R_S, and R_r. In these items, the R_S and R_r. are newly selected random numbers by the sender and receiver respectively. These random numbers will be changed every time to ensure the K_S to be created dynamically. The cluster key K_C 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.

B. Secure Token Replay Attack:

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

C. Forge Attack:

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

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 $h(h(K_S))$ from K_S, the valid $h(h(K_S))$ 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 $h(K_S)$ from received $h(h(K_S))$, the valid $h(K_S)$ can protect the sender against "garbage" data attack from an anti-node.

VII.SIMULATION RESULTS

In this section, we present the MATLAB® model on the power of X-MAC and TE2S. Here we submit the MicaZ mote node datasheet for analyzing power consumption. The MicaZ has 4 KB of RAM, 128 KB of ROM and equips with ATmega128L MCU and Chipcon CC2420 radio unit. The ATmega128L run at 8MHz alarm clock and the transmitting data charge of CC2420 is 250 kbps. We take for granted that the power supply of MicaZ is fixed at 3.0 V. Table I shows the condition and energy utilization referred to the datasheets of ATmega128L in addition to CC2420.

Devices	States	Current	Energy Consumption
ATmega128L	Active mode	5 *m*A	15 *m*W
	Idle mode	2 *m*A	6 *m*W
	Sleep mode	25 µA	0.075 *m*W
CC2420	Transmit mode (Tx)	17.4 *m*A	52.2 *m*W
	Receive mode (Rx)	19.7 *m*A	59.1 *m*W
	Idle mode	20 µA	0.06 *m*W
	Sleep mode	1 µA	0.003 *m*W

Table I. Energy State of Atmega128l and Cc2420

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

Algorithm	Plaintext (bytes)	Action	Execution Time (*ms*)	
			Atmega128	*Atmega128L*
MD5	1-26	Digest	1.473	2.946
	62-80	Digest	2.722	5.444
RC4	16	Init.	0.472	0.944
		Enc./Dec	0.086	0.172

Table II. Execution Time and Energy Consumption of Security Algorithm

In this model, the MD5 is selected as the hashing function, and the RC4 is preferred as the encryption/decryption algorithm since they are computational inexpensive and proper for sensor network. The safety measures mechanisms overhead of MD5 and RC4 on ATmega128 have been studied. The ATmega128L divide up the same hardware construction with the ATmega128, excluding the ATmega128L runs at 8MHz clock, which is a partially of the ATmega 128. As a result the execution moment in time of security algorithm of ATmega128L doubles to facilitate of ATmega128. Table II shows the implementation time and energy consumption of safety measures algorithm of ATmega128 and ATmega128L.

Parameters	Time (*ms*)
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

Table III. Protocol Parameters Values of Simulations

We assume the level of cluster key, safe token, casual number and session key is 16 bytes. The extent of ID and clock of node is implicit 2 bytes. The random number selection is making simpler as the hashed output of node ID and MCU's control. Based on these statement, the entity energy utilization of security operations is estimate. The assessment of 16 bytes protected token and hash chains can be completed in tens of sequence by the MicaZ MCU. Evaluate with thousands cycles fixed cost of security algorithms; we suppose the power of comparison is small and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

can be neglected.

The duty sequence is 4.76%. The transmitted information will be encrypted by RC4 algorithm in the new X-MAC protocol. The packet sending time is 1 packet each 5 seconds and 3 seconds. The sensor node will send out received information right after the information packet received and completed. It shows the model results under the packet sending time of 1 packet every 5 seconds and 3 seconds correspondingly. Table IV shows normalized power consumptions of unique X- MAC and the proposed protected TE$_2$S scheme.

Packet rate	Energy consumption (J/Hour)		Difference
	X-MAC	*TE$_2$S*	
1 packet / 5 seconds	24.78	25.59	3.27%
1 packet / 3 seconds	33.67	35.04	4.08%

Table IV. Normalized Energy Consumptions of Schemes

Under the package sending rate of 1 packet each 5 seconds, the proposed safe TE2S scheme enhances 3.27% in energy utilization. With the package sending time 1 packet every 3 seconds, the proposed secure TE$_2$S scheme raise 4.08% in energy utilization.

VIII.CONCLUSION

This paper proposes a cross-layer plan of energy-efficient protected system integrating the MAC procedure. No additional packet is involved in the new MAC 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. 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 TE S method. 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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 12, December 2015

[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.
[1 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.