INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW-ENERGY EFFICIENT SECURITY SCHEME FOR WIRELESS SENSOR NETWORKS

APARNA S. KALASKAR[1], PROF. G. D. GULHANE[2]

1. PG student Department of Computer Science and Engineering, Shri Sant Gajanan Maharaj College of Engineering, Shegaon.
2. Department of Computer Science and Engineering, Shri Sant Gajanan Maharaj College of Engineering, Shegaon.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: WSN is one of the most forceful technologies of the current tech-savvy generation. WSN are made up of tens to potentially thousands of small, low-power sensor devices designed to sense information about their environment and then transmit that information to other network nodes or to a base station. Like other networks, sensor networks are vulnerable to malicious attack. One of the most valuable asset is the power supply, security and energy efficiency are critical problem in WSN. In power consumption related attacks an attacker tries to exhaust the wireless device's power supply and it may degrade the lifetime of the network. The current design of MAC protocol are insufficient to protect the WSNs from power consumption attacks in MAC layer. This paper will present an energy-efficient security scheme against power exhausting attack.

Keywords: Wireless sensor networks (WSNs), Energy efficiency, Power exhausting attack, secure scheme

Corresponding Author: MS. APARNA S. KALASKAR

PAPER-QR CODE

Access Online On:

www.ijpret.com

How to Cite This Article:

Aparna S. Kalaskar, IJPRET, 2016; Volume 4 (9): 320-327

INTRODUCTION

Wireless Sensor Networks (WSNs) experienced a rapid growth with a huge interest from both academia and industry. WSNs have great long-term economic potential, ability to transform our lives and pose many new system-building challenges. Sensor networks pose a number of new conceptual and optimization problems such as data integrity and confidentiality, power consumption, routing, identity, privacy, and service availability. One of the most valuable asset in wireless network is the power supply. In power consumption related attacks an attacker tries to exhaust the wireless device's power supply and it may degrade the lifetime of the network. A worst case scenario may even collapse the network communication, especially the denial-of-sleep attacks, which can shorten the life of WSN's rapidly[1-3]. Duty cycle based protocol is one of the major schemes in energy conservation of WSN's. The primary objective of duty cycling is to reduce the energy consumption of motes and to increase the overall network longevity as a consequence. The sensor nodes are switched between awake/active and sleep state periodically and these nodes enter sleep mode after certain idle period, in the duty cycle based WSN MAC protocol[3]. B-MAC[2] sometimes reoffered to as Low Power Listening (LPL) based on WSN MAC protocol consumes the major energy of both sender and receiver, this also decouples the sender and receiver with time synchronization as an asynchronous protocol. Duty cycle scheme can be classified into two types of asynchronous method: sender-initiated scheme and receiver initiated scheme. The scheme has been improved by the introduction of short preamble techniques in X-MAC. However this existing design of protocol are insufficient to protect a WSN from power exhausting attack like Deniel-of-Sleep attack[5].

The Deniel-of-Sleep is a special type of Deniel-of-Service(DoS) attack, which tries to keep the sensor node awake to consume more energy of the given power supply. Denial of sleep attacks force a sensor platform to stay awake and receive a transmitted packet. If the complete packet is encrypted, the sensor node must receive the entire packet, decrypt the header,and then determine if it is the intended receiver. The data-only encryption mode allows the node to view the header as it arrives, but the node will not be able to authenticate the sender until the packet data is decrypted. In this case, if the attacker is able to provide a legitimate source and destination, the receiver will stay awake to accept the entire packet. The link layer will then discard any packets which fail the message authentication code check. The unencrypted mode expends the same amount of energy receiving the packet, and it will pass the incoming message up to the network layer[4]. Such attack will keep the reciver awake as long as the data transmission sustain, which exhausts the battery of nodes rapidly. For this easy and fast authentication scheme is needed to integrate with MAC protocol to counter this power exhausting attack.

This paper proposes a cross layer design of secure scheme integrating the MAC protocol and a two-tier secure transmission scheme. A cross-layer design proposals from the literature based on the layers that are coupled. This design involves coupling two layer witout creating interface for runtime sharing information. The design principles and features of the proposed secure scheme are:

- Energy conservation
- Low complexity
- Mutual authentication
- Symmetric encryption
- Dynamic session key generated with challenge text
- Capability to counter the Denial-of-Sleep attack
- Integrating the MAC protocol

A two-tier secure transmission scheme. 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 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.

2. LITERATURE REVIEW & RELATED WORK

The following sections show the work done by the various researcher : In the paper [1] A. Bachir provide a comprehensive state-of-the-art study in which we thoroughly expose the prime focus of WSN MAC protocols, design guidelines that inspired these protocols, as well as drawbacks and shortcomings of the existing solutions and how existing and emerging technology will influence future solutions. In contrast to previous surveys that focused on classifying MAC protocols according to the technique being used, we provide a thematic taxonomy in which protocols are classified according to the problems dealt with. We also show that a key element in selecting a suitable solution for a particular situation is mainly driven by the statistical properties of the generated traffic.

J. Kabara[2] In this paper suggests that contention-based approaches may be helpful when the network topology is random, application requirements are not delay constrained, and there is no mechanism to ensure tight synchronization. Analysis also shows that schedule-based approaches may be more energy efficient if deployment is not random and the base stations include high-power transmitters and large energy stores which can be used to manage synchronization and schedules. Protocol designers and users benefit from standard test methods that can be applied across all communication protocols for WSN, so that protocols can be measured using the same references and units, allowing for comparison and evaluation.

R.C. Carrano[3] This paper suggests organizes the most important proposals into a taxonomy and provides insights into their strengths and weaknesses in relation to important characteristics of applications, mote's hardware and network deployments.

M. Brownfield [4] describes the denial of sleep vulnerabilities for leading wireless sensor network MAC protocols and models the catastrophic effects these attacks can have on a deployed network. The link layer denial of sleep attack exposes the necessity to consider all primary threats to every system component during the design phase to properly integrate security with functionality. The WSN link layer MAC protocol introduced in this paper, Gateway MAC, established an effective denial of sleep defense by centralizing cluster management.

M. Buettner [5] describes X-MAC, a new approach to low power communication in WSNs. X-MAC employs a strobed preamble approach by transmitting a series of short preamble packets, each containing the address of the target receiver. This paper demonstrated a lightweight algorithm for adapting X-MAC to select near-optimal sleep and listen periods. We verified that X-MAC's strobed preamble approach outperforms traditional LPL by implementing the protocol and performing an array of experiments.

V. Srivastava[6] he takes a step in that direction by presenting a survey of the literature in the area of cross-layer design, and by taking stock of the ongoing work. Suggest a definition for cross-layer design, discuss the basic types of cross-layer design with examples drawn from the literature, and categorize the initial proposals on how cross-layer interactions may be implemented then highlight some open challenges and new opportunities for cross-layer design.

K-T.Chu [7] describes a decentralized protocol for topology management in wireless sensor networks. The Adaptive Distributed Topology Control Algorithm (ADTCA) performs cluster formation and linkage using random waiting timers and local information. On the basis of the cluster-based network topology, this self-configuring technique may be applied to achieve local and global time synchronization and to provide efficient network routing.

3. METHODOLOGY

1. SECURE TOPOLOGY FORMATION STAGE:

This stage involved Secure adaptive topology control algorithm (SATCA) to form the hierarchical topology carry out in four phases: a. anti-node detection; b.cluster formation; c.key distribution; d.key renewal[8].

Phase a. Anti-Node Detection: An authenticated broadcasting mechanism is applied to identify the anti-nodes. If the sensor cannot decrypt the received message successfully then here sender is known to be an anti-node.

Phase b. Cluster Formation: The adaptive distributed topology control algorithm (ADTCA) [7] Performs the clusterhead selection and the gateway selection to form the clusters.

Phase c. Key Distribution: Two symmetric keys, a cluster key and gateway key , are distributed locally under cluster construction. A cluster key is a key shared by a clusterhead, gateway key is protection against anti-nodes that have not been found out in Phase a.

Phase d. Key Renewal: The key renewing process revokes the old keys and accomplishes the renewal of the keys. The process of key distribution is shown in fig. 1.

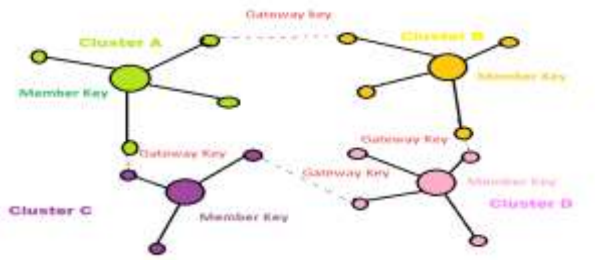

Fig. 1. Key Distribution for WSNs

2. A TWO-TIER SECURE TRANSMISSION SCHEME:

Two-tier secure transmission scheme, Design principles of this based on acknowledgement process. Two tier design can check and interrupt the attack at different check points. The combination of low complexity security process and multiple check points design can defense against attack and send the sensor node back to sleep mode as soon as possible.

In this security stage of WSN’s, 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, which suggests that the design of security scheme in upper layers may have to be coupled with the data link layer mechanism. The proposed cross-layer design, Two-Tier Energy Efficient Secure scheme(*TE_2 S)*, integrates the MAC protocol and involves coupling two layers without creating new interface for information sharing at runtime, which aims to protect the WSNs from Denial-of-Sleep attack.

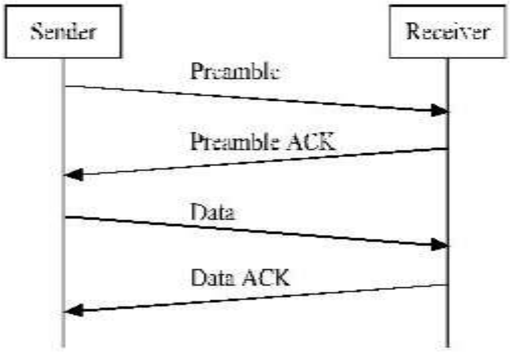

Fig. 2. Packet exchange procedure in the X-MAC protocol.

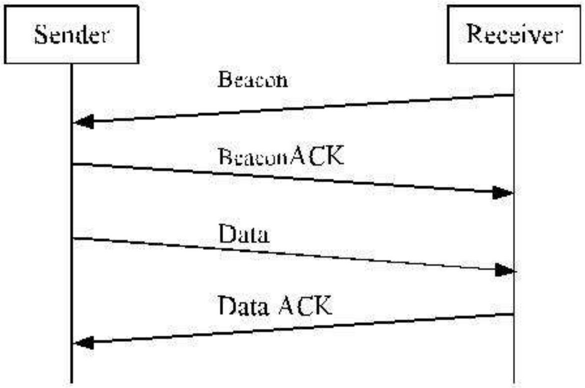

Fig. 3. Packet exchange procedure in the RI-MAC protocol

As previously known the LPL based B-MAC protocol has no ACK mechanism. The X-MAC and RI-MAC protocols are involved as the basic architectures of the proposed security scheme [5]. The procedures of packet exchange in the X-MAC and RI-MAC protocol are shown in Fig. 2 and Fig. 3, respectively

A Tier-two secure transmission scheme included two layer, 1. Tier-1, 2. Tier-2.

Tier-1: Session Key Agreement:

- Sender-Initiated Scheme
- Receiver-Initiated Scheme

Tier-2: Data transmission:

- Sender-Initiated Scheme

This Objectives are achieve the same throughput performance with less energy consumption.

3. CONCLUSION

This experiment proposes secure *TE_2 S* scheme can achieve the same throughput performance with less energy consumption. Further energy consumption of the proposed scheme under various duty cycles can be investigated to provide more extensive simulation results to support the efficiency of *TE_2 S* scheme in the later.

REFERENCES

1. 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.
2. 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.
3. 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.
4. M. Brownfield, Y. Gupta, and N. Davis, “Wireless sensor network denial of sleep attack,” in *Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop (IAW)*, New York, NY, USA, Jun. 2005, pp. 356–364.
5. 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. 4th Int. Conf. Embedded Netw. Sensor Syst. (SenSys)*, Boulder, CO, USA, 2006, pp. 307–320
6. V. Srivastava and M. Motani, “Cross-layer design: A survey and the road ahead,” *IEEE Commun. Mag.*, vol. 43, no. 12, pp. 112–119, Dec. 2005.

7. K.-T. Chu, C.-Y. Wen, Y.-C. Ouyang, and W. A. Sethares, "Adaptive distributed topology control for wireless ad-hoc sensor networks," in *Proc. Int. Conf. Sensor Technol. Appl. (SensorComm)*, Valencia, Spain, 2007, pp. 378–386

8. C.-T. Hsueh, Y.-W. Li, C.-Y. Wen, and Y.-C. Ouyang, "Secure adaptive topology control for wireless ad-hoc sensor networks," *Sensors*, vol. 10, no. 2, pp. 1251–1278, 2010.

9. C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme for power exhausting attack in hierarchical wireless sensor network," IEEE Sensors journal,vol. 15, NO 6, June 2015.

10. Y.-C. Ouyang, C.-B. Jang, and H.-T. Chen, "A secure authentication policy for UMTS and WLAN interworking," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Glasgow, U.K., Jun. 2007, pp. 1552–1557.

11. 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.