ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

Result on Enhancing Security in Wireless Sensor network through Energy Analysis Scheme

[1] Pallavi Vijay Dongardive, [2] Prof. A.U Chhajed
[1][2] Anuradha Engineering College Chikhli

***Abstract*— Wireless Sensor Networks (WSNs) growing rapidly with a huge interest from both academia and industry as they are potentially low cost and effective. WSN are made of hundreds of constraints dependent sensors for solving real world sensitive applications. The nodes are disperse over an area to watch and record the data as needed by the application and to forward same data to the center node for further observation, which may generate an alert to control the situation. As it is growing rapidly there is more demand of security, like other network ,WSN are also vulnerable to malicious attack, such as power exhausting attacks, especially the denial-of-sleep attacks. DoS attacks can exhaust the battery of the sensor node and rapidly decreases the lifespan of wireless sensor network. To save these power and to increase the lifespan of WSNs, various media access control (MAC) protocols are proposed. But the present designs are insufficient to secure the dos attacks in MAC layer. This paper will proposes the scheme which enhances the security in wireless sensor network through energy analysis scheme.**

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

I. INTRODUCTION

Wireless Sensor networks have been researched and deployed for decades which has tremendous upsurge in recent years. This is mainly attributed to the unprecedented operating conditions of wireless sensor networks (WSNs). Wireless sensor networks (WSNs) consist of hundreds or even housands of small devices each with sensing, processing, and communication capabilities to monitor the real-world nvironment. In these networks, a large number of sensor nodes are deployed to monitor a vast field, where the perational conditions are most often harsh or even hostile .They are used in many applications in military, ecological, and health-related areas, Industrial area to monitor physical or environmental conditions to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity[1][3]. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, power consumption, routing and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. The most important constraint is power supply. In this power exhausting attack attacker intentionally try to exhaust the energy of sensor node which may reduce the lifetime of network. Denial of sleep attacks (DoS attack) is recognized as one of the power exhausting attack in which tries to keep the sensor nodes awake to consume more energy of the constrained power supply. Without security mechanism fake node or anti node sends fake data to the sensor network ,as sensor node doesn't tell real preamble and fake one it processes data from anti node which keeps sensor node awake as long as the data transmission sustains, which exhausts the battery of nodes rapidly[4]. In the duty-cycle based WSN MAC protocols, the sensor nodes are switched between awake or active and sleep state periodically and after certain idle period these nodes enter sleep mode. WSNs MAC protocol uses Low Power Listening (LPL) based protocol i.e. B-MAC, in which the receiver wakes up periodically and then senses, receive and process the data send from sender .This is an asynchronous protocol. In which whenever sender want to send data it has to send data with a long permeable which can covers the speed time of sender ,this long permeable requires more energy from both sender and receiver. Duty cycles scheme classified into two i.e sender-initiated scheme X-MAC protocol and receiver initiated (RI) scheme B-MAC protocol. In this the long permeable replace by short permeable ,but current layer-2 protocol designs are insufficient to protect a WSN from Denial-of-Sleep attack[4].

In Denial-of-Sleep attack the attacker which tries to keep the sensor node awake to consume more energy of the given power supply. The Denial-of-Sleep is special type of Denial-of-Service of attack; The common method of attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. 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. In this paper, a cross layer design of secure scheme integrating the MAC protocol ,Two-Tier Energy-Efficient Secure Scheme (TE2S). the two Tier Energy-Efficient Secure Scheme (TE2 S), is proposed to protect the WSNs from the above attacks based on our preliminary frameworks[4].

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 without 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

This paper proposes 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 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.

II. LITERATURE REVIEW & RELATED WORK

The following sections show the work done by the various researcher

[1] MAC essentials for wireless sensor networks
AUTHORS: A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung
They 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. According 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.

[2] MAC protocols used by wireless sensor networks and a general method of performance evaluation
AUTHORS: J. Kabara and M. Calle
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.

[3] Survey and taxonomy of duty cycling mechanisms in wireless sensor Networks
AUTHORS: R. C. Carrano, D. Passos, L. C. S. Magalhaes, and C. V. N. Albuquerque
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.

[4] Wireless sensor network denial of sleep attack
M. Brownfield, Y. Gupta, and N. Davis,
It 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.

[5] X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks
M. Buettner, G. V. Yee, E. Anderson, and R. Han

describes X-MAC, a new approach to low power communication in WSNs. X-MAC employs a strobe 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 strobe preamble approach outperforms traditional LPL by implementing the protocol and performing an array of experiments.

[6] Cross-layer design: A survey and the road ahead
V. Srivastava and M. Motani
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.

[7] Adaptive distributed topology control for wireless ad-hoc sensor networks
K.-T. Chu, C.-Y. Wen, Y.-C. Ouyang, and W. A. Sethares
They 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.

III. SECURE TOPOLOGY FORMATION STAGE:

This stage forms the hierarchical topology in which it involves Secure adaptive topology control algorithm (SATCA) which is having four phases
(I) anti-node detection; (II) cluster formation; (III) key distribution; (IV) key renewal[4].

Phase a. Anti-Node Detection:
An authenticated broadcasting mechanism is needed for the network to make more robust. In this mechanism a plaintext message is encrypted by the pre-distributed key as the broadcasting challenge. If the sensor cannot decrypt the received message successfully, then sender will be an anti-node. hence we can find out the node and anti node.

Phase b. Cluster Formation:
The adaptive distributed topology control algorithm (ADTCA) [8] Performs the cluster head 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 are encrypted by the pre-distributed key under cluster construction. A cluster key is a key shared by a cluster head, gateway key is protection against anti-nodes that have not been found out in Phase of anti node detection.
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.

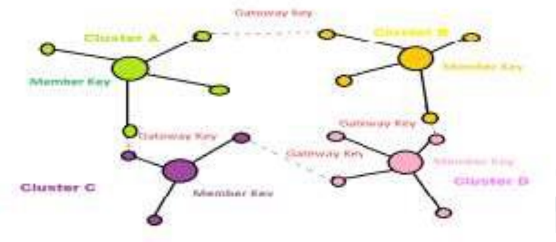


Fig. 1. System Architecture

A TWO-TIER SECURE TRANSMISSION SCHEME
After the secure topology formation stage, there is a shared secret key between the valid member nodes and cluster head of each cluster. A cluster key is a key shared by a cluster head and all its cluster members, which is mainly used for securing local broadcast messages (e.g. routing control information or sensor messages). Based on the secure cluster topology, a two-tier security scheme is performed to transmit information securely and quickly. This scheme can assist the nodes in deciding to switch into sleep mode or to keep awake as soon as possible[4]. 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[9].

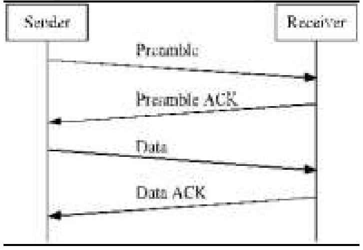


Fig. 2. Packet exchange procedure in the X-MAC protocol.

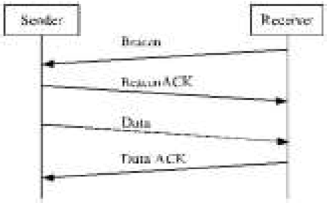


Fig. 3. Packet exchange procedure in the RI-MAC

The procedures of packet exchange in the X-MAC and RI-MAC protocol are shown in Fig. 2 and Fig. 3, respectively. The X-MAC and RIMAC protocols are involved as the basic architectures of the proposed security scheme[10].A Tier-two secure transmission scheme included two layer, 1. Tier-1, 2. Tier-2

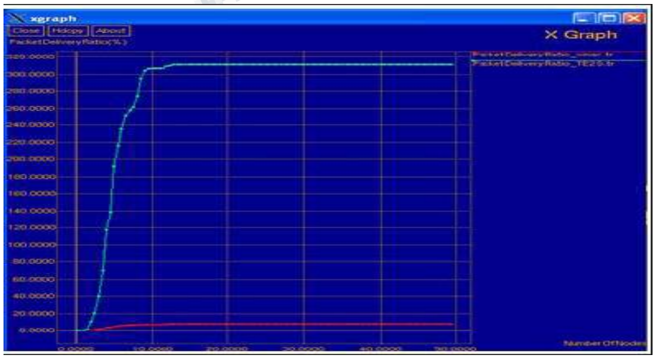
Tier-1: Session Key Agreement:
•Sender-Initiated Scheme
•Receiver-Initiated Scheme

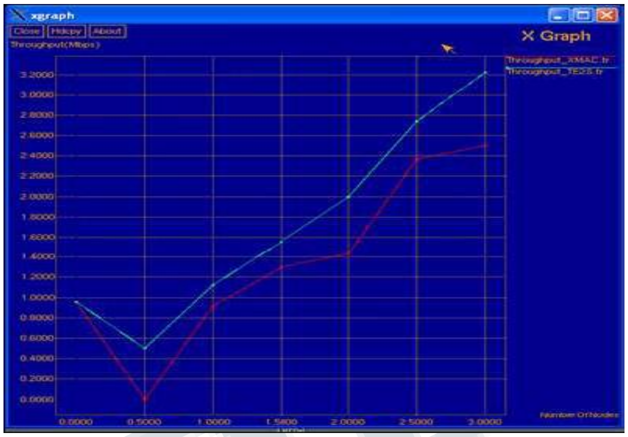
Tier-2: Data transmission:
•Sender-Initiated Scheme

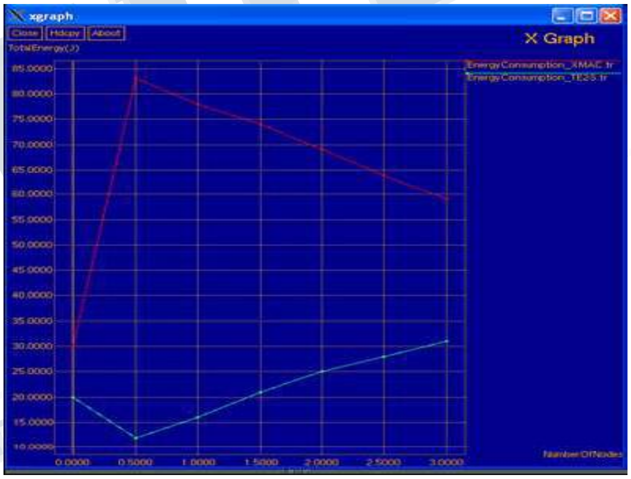
This Objectives are achieve the same throughput performance with less energy consumption.

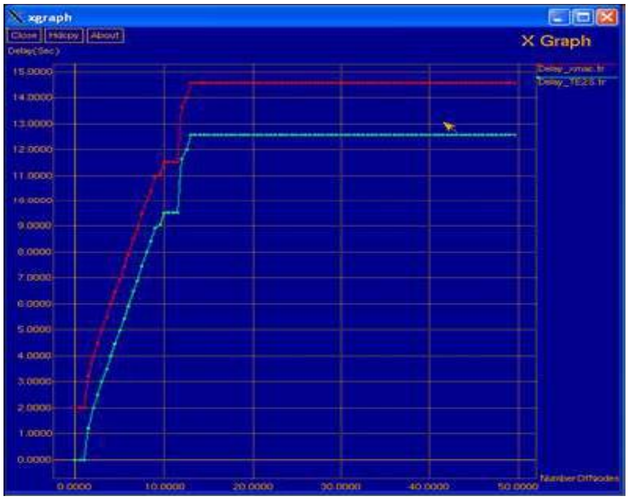
IV. RESULT

In the field of in computer science, constructed product result analysis (or CPR analysis) is a static analysis that determines which functions in a given program can return multiple results in an efficient manner. We now assess the performance of the proposed TE2S i.e Two-Tier Energy-Efficient Secure Scheme in comparison of X-MAC to show that are indeed preferable. We calculate the results with respect to time. The experiment can be conducted with four parameter, number of packet delivered , throughput, energy consumption and delay.









CONCLUSION

This paper proposes secure TE2 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 TE2 S scheme in the later.

REFERENCES

[1] MAC Essentials for Wireless Sensor Networks Abdelmalik Bachir, IEEE Member, Mischa Dohler, IEEE Senior Member Thomas Watteyne, IEEE Member, Kin K. Leung, IEEE Fellow.

[2] MAC Protocols Used byWireless Sensor Networks and a General Method of Performance Evaluation Joseph Kabara1 and Maria Calle21School of Information Sciences, University of Pittsburgh, Pittsburgh, PA 15260, USA Department of Electrical and Electronic Engineering,Universidad del Norte, Barranquilla, Colombia

[3] Security in Wireless Sensor Networks Jaydip Sen Department of Computer Science & Engineering, National Institute of Science & Technology, INDIA

[4] A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks. Ching-Tsung Hsueh, Chih-Yu Wen, Member, IEEE, and Yen-Chieh Ouyang, Member, IEEE

[5] X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks M. Buettner, G. V. Yee, E. Anderson, and R. Han.

[6] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, “High-speed digital-to-RF converter,” U.S. Patent 5 668 842, Sept. 16, 1997.

[7] 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.

[8] 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

[9] Aparna s. Kalaskar, prof. G.d.gulhane “result on energy efficient security scheme for wireless sensor network” Department of Computer Science & Engg., Dr. R. G. I. T. & R., Amravati.

[10]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