INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

RESULT ON ENERGY EFFICIENT SECURITY SCHEME FOR WIRELESS SENSOR NETWORKS

APARNA S. KALASKAR, PROF. G.D.GULHANE

Department of Computer Science & Engg., Dr. R. G. I. T. & R., Amravati.

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

Abstract: WSN is one of the most widely used network. Now a days WSN's has been grown tremendously in the applications, resulted the demand of a heavy, consistent security mechanism. Security and energy efficiency are critical concerns in wireless sensor network (WSN) design. WSN have some issues, one of the most valuable issue is the power supply. There is a need to develop energy-efficient secure scheme against power exhausting attacks, especially the denial-of-sleep attacks. 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

Access Online On:

www.ijpret.com

How to Cite This Article:

Aparna S. Kalaskar, IJPRET, 2016; Volume 4(9): 1633-1641

PAPER-QR CODE

INTRODUCTION

Securing wireless sensor networks (WSNs) adds more challenges to the research. This is because WSN properties make it harder to be secured than other types of networks. In WSNs, applying a high security level imposes more resource and decreases the energy efficiency of network. Sensor networks are vulnerable to several malicious attacks. Since sensor batteries are severely limited, Denial of sleep attacks (DS attack) is recognized as one of the most serious threats. The Denial of sleep attack is a specific type of denial-of-service (DoS) attack that targets a battery-powered device's power supply in an effort to exhaust this constrained resource and reduce the network life time. Indeed, this attack tries to break in the device's power management system to reduce the opportunities to transition into lower power states.

This attack tries to keep the sensor nodes awake to consume more energy of considered power supply and anti-node can send fake data packets to sensor node of unprotected WSNs to initiate unnecessary transmissions repeatedly. Although various media access control (MAC) protocols have been proposed to save the power and extend the lifetime of WSNs, the existing designs of MAC protocol are insufficient to protect the WSNs from denial-of-sleep attacks in MAC layer**.**

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. In this paper, a cross-layer design of secure scheme integrating the MAC protocol. Two-Tier Energy-Efficient Secure Scheme (TE_2 S), is proposed to protect the WSNs from the above attacks based on our preliminary frameworks. To secure network nodes from denial of sleep attacks, proposed a cross layer energy efficient security mechanism where the cross layer interaction is heavily exploited. This approach reuses mainly the already available data generated by network, Mac layers to provide security scheme for network node.

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.

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.

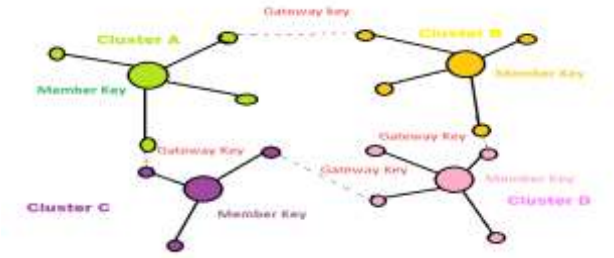


Fig. 1. System Architecture

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.

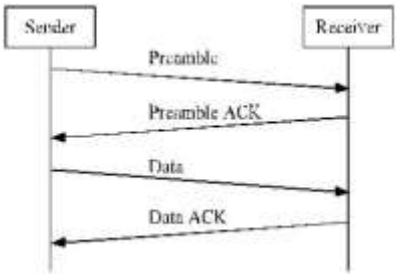


Fig. 2. Packet exchange procedure in the X-MAC protocol.

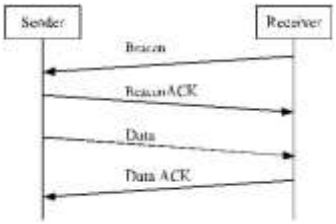


Fig. 3. Packet exchange procedure in the RI-MAC

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:

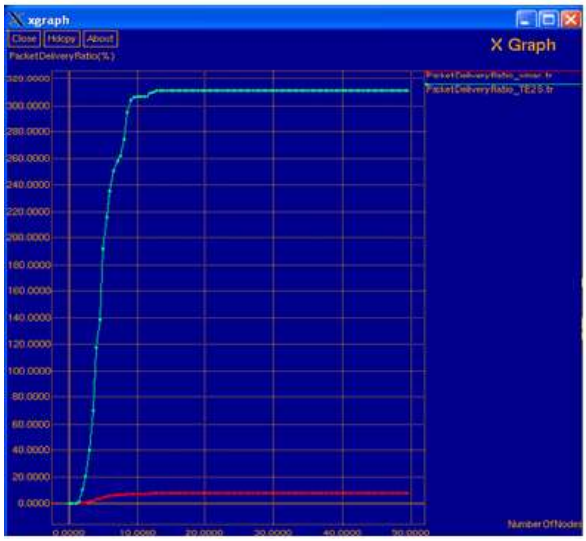
- Sender-Initiated Scheme

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

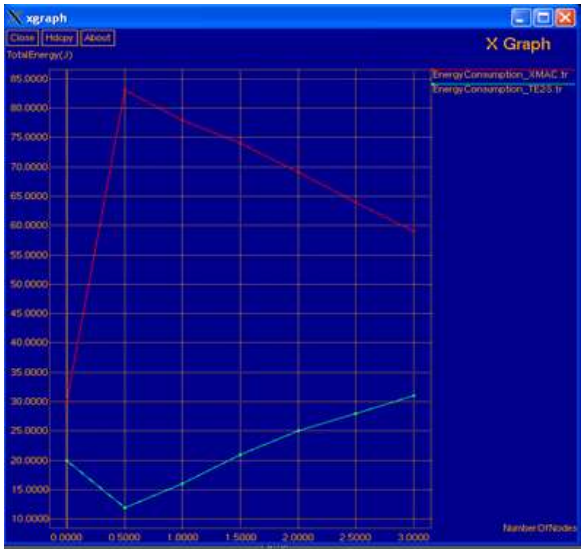
4. RESULT

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 comparision 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.




xgraph
Close
Hdcpy
About
X Graph
Throughput(MBps)
Throughput_XMAC.tr
Throughput_TE2S.tr
3.2000
3.0000
2.8000
2.6000
2.4000
2.2000
2.0000
1.8000
1.6000
1.4000
1.2000
1.0000
0.8000
0.6000
0.4000
0.2000
0.0000
0.0000
0.5000
1.0000
1.5000
2.0000
2.5000
3.0000
Number Of Nodes


xgraph
Close
Hdcpy
About
X Graph
TotalEnergy(J)
Energy Consumption_XMAC.tr
Energy Consumption_TE2S.tr
85.0000
80.0000
75.0000
70.0000
65.0000
60.0000
55.0000
50.0000
45.0000
40.0000
35.0000
30.0000
25.0000
20.0000
15.0000
10.0000
0.0000
0.5000
1.0000
1.5000
2.0000
2.5000
3.0000
Number Of Nodes

4. 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.