A SCHEMA AGAINST HIERARCHICAL WIRELESS SENSOR NETWORKS POWER ATTACK

Nirmala S 1, Ambika Doddamani 2

1Associate professor Department of CSE AMCEC Bangalore, India
2M.TECH Student Department of CSE AMCEC Bangalore, India

ABSTRACT:

Security and energy efficiency are critical concerns in wireless sensor network (WSN) design. This paper aims to develop an energy-efficient secure scheme against power exhausting attacks, especially the denial-of-sleep attacks, which can shorten the lifetime of WSNs rapidly. 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. This is attributed to the fact that the well-known security mechanisms usually awake the sensor nodes before these nodes are allowed to execute the security processes. Therefore, the practical design is to simplify the authenticating process in order to reduce the energy consumption of sensor nodes and enhance the performance of the MAC protocol in countering the power exhausting attacks. This paper proposes a cross-layer design of secure scheme integrating the MAC protocol. The analyses show that the proposed scheme can counter the replay attack and forge attack in an energy-efficient way. The detailed analysis of energy distribution shows a reasonable decision rule of coordination between energy conservation and security requirements for WSNs.

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

INTRODUCTION

To save energy and expand the lifetime of WSNs, a few plans have been proposed. In the Low Power Listening (LPL) based WSN MAC convention, for example, In B-MAC, at the point when the sender needs to send information, it sends a long preamble to cover the sleep period to guarantee the receiver awakening and detecting. The LPL based MAC convention is a no concurrent convention, which decouples the sender and receiver with time synchronization. For example, the X-MAC convention is one of the sender initiated schema.
to enhance B-MAC convention by replacing the long preamble with short preamble, which permits the receiver to send ACK back to the sender when it detects the preface. The RI-MAC convention is one of the receiver initiated schema to minimize the channel inhabitance time of a couple of a sender and receiver, which permits the sender to send information to the beneficiary when it detects the reference point.

The energy preservation is one of the real objectives of WSN outline. The Denial-of-Sleep is one of the force depleting attacks of WSNs. This attack is an extraordinary kind of Denial-of-Service (DoS) attack, which tries to keep the sensor node alert to devour more energy of the compelled power supply. A hostile to node can send fake information parcels to sensor node of unprotected WSNs to start pointless transmissions over and over. Without security component, a hostile to node can telecast a fake prelude every now and again in the sender-started plans.

In the event that the beneficiary can't tell the genuine preface and the fake one, the receiver will get and prepare the information from the counter node. Such attack will keep the receiver alert the length of the information transmission supports, which depletes the battery of node quickly. In addition, an against node can replay a fake introduction ACK to the sender. In this way, the sender will begin to send the information to the counter node yet it will never get the right information ACK. So also, the sender might send information over and over and depletes the battery of node quickly. In receiver initiated schema, a hostile to node can telecast a "fake reference point" to cheat sender to handle and send the information to the counter node however it will never get the right information ACK.

The functional configuration is to improve the security process when enduring the force depleting attacks. The outline of security plan in upper layers might be combined with the settled information join layer system. In this paper, a cross layer configuration of secure plan incorporating the MAC convention, Two-Tier Energy-Efficient Secure Scheme (TE2S), is proposed to shield the WSNs from the above attacks in light of our preparatory systems.

[2] EXISTING SYSTEM
The B-MAC is a LPL based WSN MAC protocol which decouples the sender and receiver with time synchronization. The receiver awakens intermittently to sense the introduction from the sender and afterward to get and prepare the information. At the point when the sender needs to send information, it sends a long preamble to cover the sleep period to guarantee the beneficiary awakening and detecting. Figure 1 demonstrates the course of events of B-MAC convention. The B-MAC convention has no ACKs and the receiver needs to listen and to sit tight for the long preamble finished from the sender. This long preamble outline of LPL based convention devours the real vitality of both sender and receiver. The X-MAC convention enhances LPL based B-MAC convention by supplanting the long preface with short preludes. This short preamble outline decreases the energy consumption of both the sender and receiver.
[3] PROPOSED SYSTEM

This paper proposes a two-level secure transmission plan. This plan utilizes the hash-chain to create the dynamic session key, which can be utilized for common confirmation and the symmetric encryption key. The main calculations of element session key are the hash capacities, for example, MD5 or SHA-1, which are extremely straightforward and quick. By coordinating with MAC convention, there is no additional bundle contrasted and the current MAC plans. The two-level outline can check and interfere with the attacks at various check points. The mix of low complexity security process and multiple check point can resistance against attacks and send the sensor node back to rest mode at the earliest opportunity. The security investigation demonstrates that this plan can counter the replay attack and forge attack, and the energy analysis demonstrates that this plan is energy effective too.

[3.1] SECURE TOPOLOGY FORMATION STAGE

The hierarchical topology in four phases: (I) anti-node detection; (II) cluster formation; (III) key distribution; (IV) key renewal

Phase I: Anti-Node Detection

An authenticated broadcasting mechanism, may be needed in this phase. In the authenticated broadcasting mechanism, a plaintext “Hello” message is encrypted by the pre-distributed key as the broadcasting challenge. If the sensor cannot decrypt the received message successfully, the sender is said to be an anti-node. Thus, the normal nodes and the anti-nodes can be differentiated. Therefore, we keep on the network topology without anti-nodes in order to make the network safe.

Phase II: Cluster Formation

When sensors are first deployed into the network graph partitioning algorithm is used to partition the sensors into the clusters

1) Cluster head Selection:
   The sensors that hear many neighbors are good candidates for initiating new clusters; those with few neighbors should choose to wait. Sensors update their neighbor information

2) Gateway Selection:
   To interconnect two adjacent non-overlapping clusters, one cluster member from each cluster must become a gateway.

Phase III: Key Distribution

In this phase, two symmetric shared keys, a cluster key and a gateway key, are encrypted by the pre-distributed key and are distributed locally. A cluster key is a key shared
by a cluster head and all its cluster members, which is mainly used for securing locally broadcast messages

Phase IV: Key Renewal

Using the same encryption key for extended periods may incur a cryptanalysis risk. To protect the sensor network and prevent the adversary from getting the keys, key renewing may be necessary.

[3.2] DESIGN PRINCIPLES OF TE2S

Based on the secure cluster topology, a two-tier security scheme is performed to transmit information securely and quickly. In this work, the X-MAC and RI-MAC protocols are involved as the basic architectures of the proposed security scheme. The procedures of packet exchange in the X-MAC and RI-MAC protocol are shown in Figure 2 and Figure 3, respectively.

![Figure 2. Packet Exchange Procedure In X MAC Protocol](image1)

![Figure 3. Packet Exchange Procedure In R1 MAC Protocol](image2)

**Tier-1: Session Key Agreement**

The detailed implementations with session key agreement of the sender-initiated scheme and that of the receiver-initiated scheme processes are described as follows.

**Sender-Initiated Scheme:**

Step 1: The sender selects a random number R 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).
Step 2: The sender sends its ID (IDs), receiver’s ID (IDs), secure token and random number R 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 Rs and computes the session key \( K_s = h(K_c|Rs|Rr) \). The receiver also computes the hash chain \( h(K_s) \) and \( h(h(K_s)) \).

Step 4: The receiver sends the \( h(h(K_s)) \) and random number Rr as the ACK.

Step 5: The sender computes the session key \( K_s = h(K_c|Rs|Rr) \) and the hash chain \( h(K) \) and \( h(h(K_s)) \). The sender then verifies the \( h(h(K_s)) \). If the \( h(h(K_s)) \) is not valid, the sender will not send the data.

Receiver-Initiated Scheme:

Step 1: The receiver selects a random number R and computes the secure token (i.e. \( Token = h(K_c| Rr) \), 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 as the beacon.

Step 3: The sender verifies the secure token. If the token is not valid, the sender goes back to beacon listen mode. If the token is valid, then sender selects a random number R key \( K_s = h(K_c|Rs|Rr) \). The sender also computes the hash chain \( h(K_s) \) and \( h(h(K_s)) \).

Step 4: The sender sends the \( h(h(K_s)) \) and random number Rs as the ACK.

Step 5: The receiver computes the session key \( K_s = h(K_c|Rs|Rr) \) and the hash chain \( h(K) \) and \( h(h(K_s)) \). The receiver then verifies the \( h(h(K_s)) \). If the \( h(h(K_s)) \) is not valid, the receiver will go back to sleep mode immediately.

Tier-2: Data Transmission

With the new created dynamic session key \( K_s \), the sender can encrypt the transmission data via symmetric encryption.

Step 1: The sender sends the \( h(K_s) \) and \( E_{K_s}(DATA |MACKs(DATA)) \) to receiver. The \( E_{K_s}(x) \) denotes encrypts x by using symmetric algorithm with key \( K_s \) The \( MACKs(DATA) \) denotes the message authentication function with key \( K_s \), where DATA is the input message.

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

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

[6] CONCLUSION

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 energy analysis shows that this scheme is efficient in
both sender-initiated scheme and receiver-initiated scheme. The overall results show that the proposed secure $TE_2S$ 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 $TE_2S$ scheme in the future.

REFERENCES


Author[s] brief Introduction

Nirmala S, Associate professor, Computer Science and Engineering, AMC Engineering College, Bangalore, India, E-mail: esthernirmala70jc@yahoo.com

Ambika Doddamani, Student, Computer Science and Engineering, AMC Engineering College, Bangalore, India, E-mail: ambikadoddamani@yahoo.com

Corresponding Address-

Ambika Doddamani,om sai ram pg ,opposite to Apollo pharmacy ,near bennergattha road,Arkeri. Pin code 560076
Phone no. 7829930915

Nirmala S and Ambika Doddamani