International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

CONSERVATION OF BATTERY POWER BY ALLEVIATING DOS ATTACKS IN WIRELESS SENSOR NETWORKS

Arpitha R , Chaitra M

Department of Information Science and Engineering,
THE NATIONAL INSTITUTE OF ENGINEERING,
Mysuru 570008, Karnataka, India

Abstract - *Sensor nodes which are building blocks of Sensor networks get their energy from battery resources whose lifespan is of major concern. As sensors are used to monitor sensitive areas, security and energy efficiency is essential consideration when designing wireless sensor networks (WSNs). The Denial-of-Sleep attack is a specific type of denial-of-service (DoS) attack that targets a battery-powered device which results in quick exhaustion of this constrained resource. To implement minimum power consumption, sensor networks periodically place sensor nodes to sleep. This is achieved by using the media access control (MAC) protocols. These protocols are designed in such a way that they reduce the energy consumption of sensor nodes by keeping the antenna in sleep mode as much as possible. This leads to power saving. The MAC protocols change the sleep time based on the type of communication required. However, malicious nodes can be introduced in the network and these attackers use their information about the MAC protocol, by manipulating the sleep time of the node, so that life time of the node reduces. This paper, addresses the Denial of sleep attack in WSN while at the same time proposing a scheme for authenticating the new nodes which try to change the sleep schedule of the nodes. Only transmissions from valid nodes are accepted. The paper presents a detailed analysis for various scenarios and also analyzes the performance while implementing this secure authentication.*

Key Words: **Sensors, Denial of Service, Denial of Sleep, Power Exhaustion, Media Access Control (MAC) Protocol.**

1. INTRODUCTION

Wireless Sensor Networks (WSNs) can be used to monitor environments, and therefore have broad range of interesting applications. The applications which may use WSN can be of sensitive nature and therefore might require enhanced secured environment. The Sensor nodes get their power from batteries. Since the sensor nodes are deployed in harsh environment they cannot be recharged. Due to unattended deployment and inability of recharging, the power consumption of the nodes should be optimal. Numerous schemes are being proposed to extend lifetime, to save energy and also provide security in WSN. Duty cycle [1] based approach is one among the scheme used to conserve the energy in a better and efficient manner. In duty cycle nodes are made to awake periodically to sense preamble from sleep to active, active to idle, idle to sleep mode. When a data is being sent at sender node in the form of preamble, a very long preamble is sent in order to overcome the sleep period. Both sender and receiver are synchronized with time. Depending on the different initiator, the duty cycle scheme can be classified into two types: Sender Initiated Scheme and Receiver Initiated Scheme. B-MAC and X-MAC are sender initiated and RI-MAC is of receiver initiated schemes. In the B-MAC (media access control) protocol a long preamble is being sent which is replaced by short preamble in X-MAC (media access control) protocol. The RI MAC (media access control) protocol will still reduce the energy consumption by sending acknowledgment to sender. RI-MAC protocol decreases the channel occupying period for both sender and receiver.

[2]The Denial-of Sleep attack is one of the power exhausting attacks which tries to keep the sensor nodes awake to consume more energy of the constrained power supply. It is hard to replace those sensors which fail on account of their battery drainage, and also without security mechanism, an anti-node can broadcast a fake preamble frequently. If the receiver cannot differentiate between the real preamble and the fake one, the receiver will receive and process the data from the anti-node. Such attack will keep the receiver awake as long as the data transmission sustains, which exhausts the battery of nodes rapidly. Moreover, an anti-node can replay a fake preamble ACK to the sender. Thus, the sender will start to send the data to the anti-node but it will never receive the right data ACK. Similarly, the sender may send data

repeatedly and exhausts the battery of node rapidly. Thus to effectively increase life of individual sensor nodes and in turn the whole sensor network the battery charge carried by these nodes must be conserved . Hence the sender and receiver need mutual authentication schemes to counter such attacks If we fail to stop the attack, the network lifetime can be reduced from months or years to days . To prevent this attack we have to authenticate nodes which are going to change the sleep time of the nodes so only synchronization messages coming from authenticated nodes are accepted.

The wireless sensor networks prefer the symmetric algorithm to avoid the complicated computing and heavy energy consumption which is depicted in Fig.1. But the encrypted data makes the battery exhaustion even worse under Denial-of-Sleep attack. The anti-node can send the encrypted "fake" data to receiver. This attack forces the receiver to decrypt the data. Before the receiver identifies that the data is "fake", the receiver consumes more power to receive and decrypt data.

These processes also keep sensor nodes awake longer. An easy and fast mutual authentication scheme is needed to integrate with MAC protocol to counter the encrypted "fake" data attack. In this paper, a cross-layer design of secure scheme integrating the MAC protocol, Two-Tier Energy-Efficient Secure Scheme (TE2S), is proposed to protect the WSNs from the above attacks. The design aim is to simplify the security process when suffering the power exhausting attacks. 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 only computations of dynamic session key are the hash functions which are simple and fast. This scheme can counter the replay attack and forge attack, and also shows that this scheme is energy efficient as well[3].

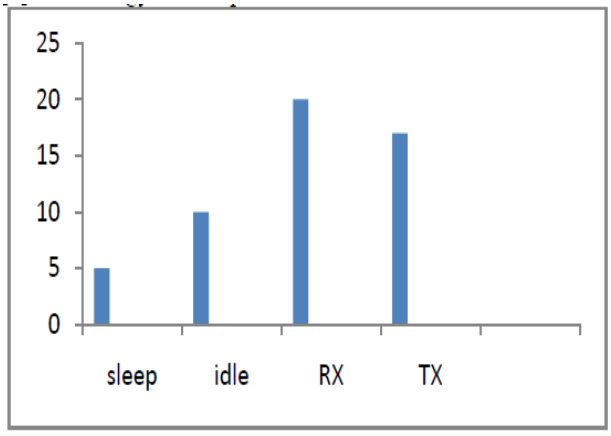


Fig. 1. Energy Consumption

2. EXISTING SYSTEM:

The B-MAC and X-MAC are sender initiated, Low Power Listening (LPL) based MAC protocol in which the receiver wakes up periodically to sense the preamble from the sender and then to receive and process the data.

2.1. B-MAC

The sender will send the long preamble whenever it has some data to send, to cover the sleep period to ensure that the receiver is up and sensing .As B-MAC protocol has no ACKs, the receiver has to listen and wait for the long preamble ended from the sender. This long preamble concept will consume lots of energy from both sender and the receiver. Fig 2 shows the timeline of the protocol.

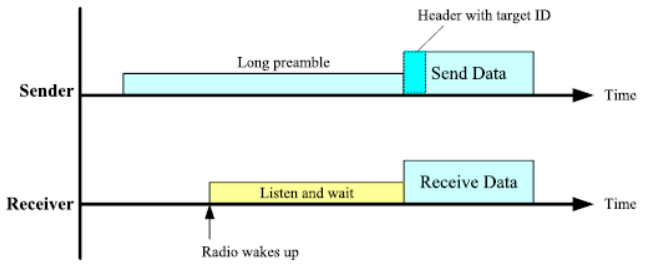


Fig. 2. Timeline of B-MAC Protocol

2.2. X-MAC

When sensor node has a packets to send to head node , it repeatedly sends the small preambles for a maximum of one duty-cycle period. When head node wakes up it will receive the preamble and send back an acknowledgement packet[4]. Upon receiving the acknowledgment, sensor node knows that its one of the preambles has successfully reached the head node, and then it sends the data packet. Fig.3. shows the Timeline of X-MAC protocol. Head node goes back to sleep if it does not hear any data packets destined to itself for the duration equal to the wake-up period. If there is additional data to send to head node, sensor node will immediately try to transmit the data as well. Though there is no sender and head node will not hear any data packet destined to itself when it is in wake up mode, head node will just go back to sleep after the wake-up period until the next polling interval. Note that if the sender cannot delivery the packet within one duty-cycle period, it stops and signals FAIL to the user application.

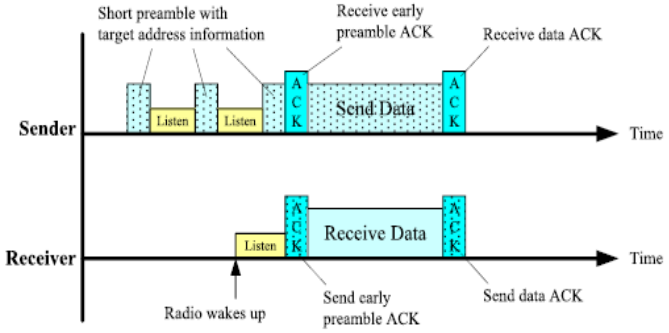


Fig. 3. Timeline of X-MAC Protocol.

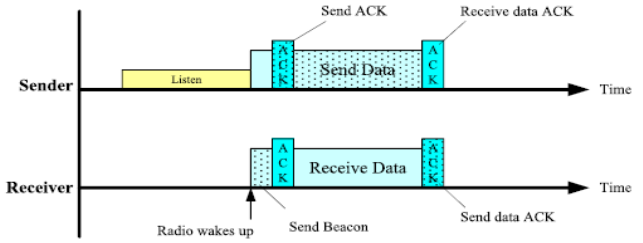


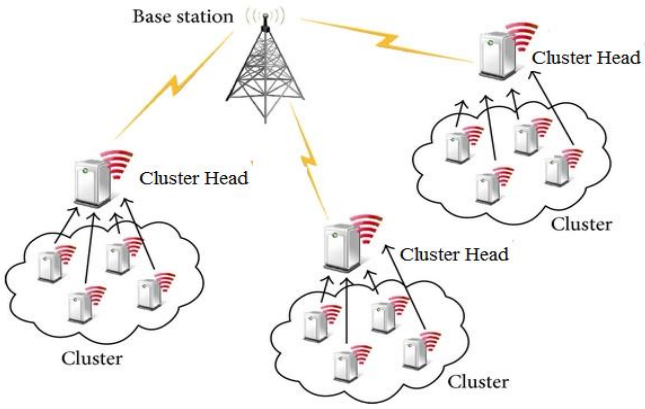
Fig. 4. Timeline of X-MAC Protocol.

3. PROPOSED SYSTEM:

3.1. RI-MAC

In Ri-MAC the head node broadcasts a beacon notifying its sensor nodes that it is ready to receive data packets when it wakes up. The beacon carries the maximum back-off value tmax. When sensor node that has data to send, receives the beacon, it first picks a random back-off time t, between 0 and tmax ms. Sensor Node then waits for this random amount of time (tms). After tms, Sensor node sends the pending data packet. Upon receiving the data packet, head node sends an acknowledgment packet that contains the data packet sequence number and also tmax. The sequence number in the acknowledgment packet informs sensor node about the successful delivery, and sensor node stays awake until it hears a acknowledgement from the receiver node. The beacon from head node initiates the data transmissions. Sensor node goes to sleep if it has no more pending data packets. Fig. 4 Shows the Timeline of RI-MAC protocol. The tmax in the acknowledgment packet is used to initiate new data transfer. If head node does not receive any incoming data packets before tmax expires, it goes back to sleep until the next scheduled wake-up time. When multiple senders exist, packet collisions can happen. For example, both S1 and S2 want to send packets to head node, but they randomly select close back-off times. If head node detects packet collision on the channel, it broadcasts a new beacon with a larger tmax after the previous tmax expires. By having a larger tmax for the next period, Ri-MAC intends increase the probability of multiple senders selecting back-off times farther away. Note that if the sender cannot deliver the packet within one duty-cycle period, it stops and signals FAIL to the user application.

4. SYSTEM ARCHITECTURE:



5. CONCLUSION:

Security and energy efficiency is the most important concerns in wireless sensor networks (WSNs) designing, since they are prostrate to different types of network attacks and intrusion. The main principle of project is to identify the malicious node and collect the details of the attacker. The MAC protocol tries to reduce energy consumption of sensor nodes by keeping the antenna in sleep mode. The proposed method provides strong authentication which defends denial of sleep attack and triggers the defending mechanism only in the area of attack where the firewalls prevents the attacker from performing the task. The above scheme is effective at transmitter begin side and receiver begin side. The proposed system can defense against attacks like forge attack, replay attack and make the sensor nodes return to sleep mode as early as possible to save energy.

REFERENCE

[1] "A Secure Scheme for Power Exhausting Attacks in Wireless Sensor Networks" Ching-Tsung Hsueh, Chih-Yu Wen and Yen-Chieh Ouyang Department of Electrical Engineering & Graduate Institute of Communication Engineering National Chung Hsing University Taichung, Taiwan 40227

[2] "Tees-Two-Tier Energy Efficient Secure Scheme For Increased Network Performance In Wireless Sensor Networks", Veena M kanthi. IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India

[3] Mechanisms for Detecting and Preventing Denial of Sleep Attacks and Strengthening Signals in Wireless Sensor Networks Chandrakala. P. Goudar1, Shubhada. S. Kulkarni2 1P G Student, Gogte Institute of Technology, Belagavi, Karnataka, India 2Asst Prof, Dept of C S E, Gogte Institute of Technology, Belagavi, Karnataka, India

[4] CS 450: Homework 3 ,Implementation and Comparison of X-MAC and Ri-MAC