DEFENDING AGAINST DENIAL OF SLEEP ATTACK IN B-MAC PROTOCOL IN WIRELESS SENSOR NETWORK

Manju.V.C. [1], **Sasi Kumar.** [2]

[1]Research Scholar, Kerala University, India
Email: [1]manju_tvm@yahoo.com

Abstract

A wireless sensor networks is a wireless network organized with huge number of sensor nodes with specialized sensors that can monitor various physical attributes such as temperature, pressure, vibration, sound. Sensor nodes are powered up with batteries. Due to unattended nature of deployment, the sensor nodes cannot be recharged again. In this condition the nodes must optimally consume power. Various protocols are designed to reduce the energy consumption of sensor nodes by keeping the antenna in sleep mode 90% of time, so that power is saved. MAC protocols are designed to adaptively vary the sleep time based on the communication need. But attackers use their knowledge of their underlying MAC protocol, to reduce the sleep time of the node, so that life time of node reduces. Here we study the B-MAC protocol and the vulnerabilities in the B-MAC protocol and propose a solution to defend the B-MAC protocol against denial of sleep problem.

Key words: security; sensor networks; denial of sleep attack; MAC protocols: B MAC.

I. INTRODUCTION

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. Research involving these devices has proposed a wide range of applications, to include atmospheric monitoring, wildlife tracking, physical perimeter intrusion detection, medical monitoring, homeland security, nuclear, biological, and chemical (NBC) monitoring, and a wide range of military applications

MAC layer protocols designed for WSNs use various algorithms to save battery power by placing the radio in low-power modes when not actively sending or receiving data. Table 1 illustrates the importance of maximizing nodes sleep ratio because transmit and receive power can be up to three orders of magnitude greater than the sleep power. The disparity between receive cost and sleep cost leads to an exponential increase in network lifetime as sleep time increases, suggesting that an attack that decreases sleep time by even a few percentage points can have a dramatic impact on network lifetime. The amount of energy that can be saved depends largely on the MAC protocol's ability to overcome the radio's four primary sources of energy loss: collisions, control packet overhead, overheating and idle listening.

Table 1. Node sleep ratio

		Mica 2™ [21]		Tmote™ Sky [22]	
power draw	Receive	36.81 mW		64.68 mW	
	Transmit	87.90 mW		55.20 mW	
	Sleep	0.09 mW		0.114 mW	
RAM		4 KB		10 KB	
Program memory		128 KB		48 KB	
RF transceiver		CC 1000		CC 2420	
Data Rate		76.8 kbps		250 kbps	
Sleep to rX transition		2.45 ms	0.095 mW	3.13 ms	0.018 mW
RX/TX transition		0.25 ms	0.016 mW	1.52 ms	0.009 mW
RX to sleep transition		0.10 ms	0.002 mW	2.16 ms	0.012 mW

A node's radio consumes the same amount of power simply monitoring the channel as it does when it is receiving data. If an attack can make a node listen even when there is no traffic destined for it, power is wasted.

B-MAC uses a technique called low-power listening (LPL) to reduce energy consumption. In low-power listening, nodes awaken briefly at a fixed interval and check the wireless channel for valid preamble bytes that indicate a pending data transmission from another node. A node with data to send transmits a preamble that is longer than the interval between receiver samplings to ensure that all nearby nodes have the opportunity to detect the preamble and receive the subsequent data packet.

In B-MAC, the condition for the node to be awake is it must sense the preamble during the time of low power awake, so any attacker can exploit this behavior and make the sensor node to be awake for a long period of time, reducing it energy and decreasing the life time of the network. In this paper, we will propose a solution to defend this attack in the B-MAC protocol.

II. LITERATURE SURVEY

In the literature survey, we explore the features in B-MAC which makes it vulnerable to denial of sleep attack and the existing solution to solve it.

B-MAC is a carrier sense media access protocol for wireless sensor networks that provides a flexible interface to obtain ultra-low power operation, effective collision avoidance, and high channel utilization [2]. To achieve low power operation, B-MAC employs an adaptive preamble sampling scheme to reduce duty cycle and minimize idle listening. B-MAC supports on-the-fly reconfiguration and provides bidirectional interfaces for system services to optimize performance, whether it be for throughput, latency, or power conservation

B-MAC duty cycles the radio through periodic channel sampling that is called Low Power Listening (LPL). Each time the node wakes up, it turns on the radio and checks for activity. If activity is detected, the node powers up and stay awake for the time required to receive the incoming packet. After reception, the node returns to sleep. If no packet is received (a false positive), a timeout forces the node back to sleep. Accurate channel assessment (CCA) is critical to achieving low power operation with this method. Noise floor estimation of B-MAC is used not only for finding a clear channel on transmission but also for determining if the channel is active during LPL. False positives in the CCA algorithm (such as those caused by thresholding) severely affect the duty cycle of LPL due to increased idle listening.

To reliably receive data, the preamble length is matched to the interval that the channel is checked for activity. If the channel is checked every 100 ms, the preamble must be at least 100 ms long for a node to wake up, detect activity on the channel, receive the preamble, and then receive the message. Idle listening occurs when the node wakes up to sample the channel and there is no activity. The interval between LPL samples is maximized so that the time spent sampling the channel is minimized.

Advantage of B-MAC is that Idle Listening is reduced to a minimum. It has a better overall performance than S-MAC.The drawback in it is that Overhearing issue is not solved. A long preamble increases the power consumption of all nodes in the sender's transmission coverage because of it. The duty cycle and thus the preamble length are tunable, but the sender and receiver should be tuned together. This requires a loose synchronization that is not easily achieved in a wireless sensor network. B-MAC is included in Tiny OS since version 1.1.3 and thus is becoming the standard MAC protocol for sensor network.

III. OVERVIEW OF PROPOSED DEFENDING SOLUTION

In this section, we present the basic idea of our proposed defending solution. Our solution consists of two parts

1. Unique preamble generation which can be authenticated.
2. Preamble valid by the sensor node to decide to stay awake.

The main loop hole in the B-MAC is that any node can generate a preamble and there is no way to authenticate the preamble is valid. Just encryption of preamble is not enough since replay attack can be launched easily. This needs a way to generate the preamble and authenticating the preamble.

Also the proposed scheme must take little time of authentication and it should not add too much network overhead. So we propose a mechanism based of Bloom filter to speed up the authentication process.

A Bloom filter, conceived by Burton Howard Bloom in 1970,[11] is a space-efficient probabilistic data structure that is used to test whether an element is a member of a set. False positive retrieval results are possible, but false negatives are not; i.e. a query returns either "inside set (may be wrong)" or "definitely not in set". Elements can be added to the set, but not removed (though this can be addressed with a counting filter). The more elements that are added to the set, the larger the probability of false positives.While risking false positives, Bloom filters have a strong space advantage over other data structures for representing sets, such as self-balancing binary search trees, tries, hash tables, or simple arrays or linked lists of the entries. Most of these require storing at least the data items themselves, which can require anywhere from a small number of bits, for small integers, to an arbitrary number of bits, such as for strings (tries are an exception, since they can share storage between elements with equal prefixes). Linked structures incur an additional linear space overhead for pointers. A Bloom filter with 1% error and an optimal value of k, in contrast, requires only about 9.6 bits per element — regardless of the size of the elements. This advantage comes partly from its compactness, inherited from arrays, and partly from its probabilistic nature. If a 1% false-positive rate seems too high, adding about 4.8 bits per element decreases it by ten times.

IV. DETAILS OF PROPOSED SECURITY MECHANISM

A. Preamble Generation

In each node a list of keys are initialized during the startup time. Each node picks up the key from the list using the current time in seconds. The key picked up hashed to n bit bloom code using the bloom filter. The key identifier and the 10 bit bloom code are sent as preamble.

The size of bloom code (*n*) can be customized according to the level of security needed. We can also use adaptive size of bloom code where the size will vary from Min < n < Max, min and max are the lower and upper bound for the bloom code.

Another important concern is that attackers attack in certain areas with more probability, so we can use a adaptive bloom code by varying the size each time and the size can be randomized between minimum and maximum size, so it becomes extremely difficult for the attacker to hack the bloom code.

The security algorithm is safe as long as the keys are not compromised. For this we suggest the use of hardware coding mechanism to maintain the keys.

The preamble goes in following format

Key ID	Bloom Code Size	Bloom Code

Key *ID* is the id of the key used. All the nodes maintain the keys in the same order, id is used to index to the key.

Time of the node is used to choose the key from all available keys. This make is necessary that all nodes are time synchronized with each other.

B. Preamble Validation

When any node receives the preamble, it authenticates the preamble. Based on it its time stamp it chooses the key and then hashes it to a bloom code. The bloom code is then validated with the bloom code in the preamble, if the bloom code are same then the preamble is valid and node can decide to stay awake and read the packet in full, if the bloom code are not same, then it is a attack, so the node goes to sleep.

C. Simulation Analysis

In order to evaluate the performance of this algorithm, this paper using Mat lab made a simulation. Divided into $100\,m \times 100\,\mathrm{m}$ area, the nodes are randomly distributed in the region. The number of nodes is varied from 20 to 150. We measured the average sleep time of node under three conditions BMAC, BMAC with attack and proposed secure BMAC with attack.

Attack is simulated by nodes frequently sending Preamble bits. Attackers are uniformly distributed over the network. We have used 10 bit bloom for authentication and distributed around 20 keys in each node.

Average sleep time was found by summing up all the nodes sleep time divided by number of nodes shown in figure 1.

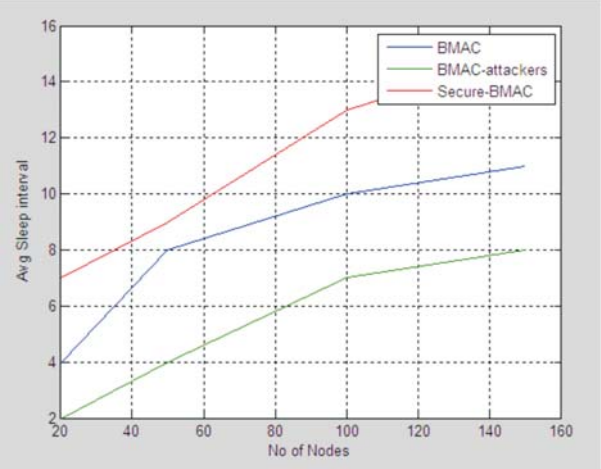

Fig. 1 Simulation Analysis for average sleep time.

We also measure the computation time taken to validate the BSYNC packets shown in figure 2.

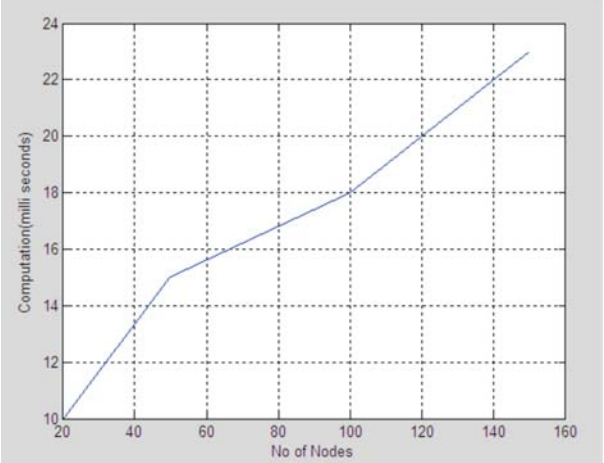

Fig. 2 Simulation Analysis for computation time taken to validate BSYNCV packets

V. CONCLUSION

In this paper, we have detailed our proposed defending mechanism against the denial of sleep attack. The proposed solution introduces the concept of securing the preamble. In the front 10 bits of preamble, security information is dynamically generated. Also we introduced a way to efficiently authenticate the preamble. With this we have secured the system against sleep attacks. By introducing randomness in the generation of preamble bits, we have also guarded against replay attacks.

REFERENCES

[1] Ye,W. Heidemann J. , and Estrin D., 2004 "Medium access control with coordinated adaptive sleeping for wireless sensor networks," IEEE/ACM Transactions on Networking, vol. 12, no. 3, pp. 493–506,

[2] VanDam T. and Langendoen K., 2003 "An adaptive energy-efficient MAC protocol for wireless sensor networks," in First ACM International Conference on Embedded Networked Sensor Systems, pp. 171–180,

[3] PolastreJ., Hill J., and Culler D., 2004. "Versatile low power media access for wireless sensor networks," in Second ACM International Conference on Embedded Networked Sensor Systems, pp. 95–107,

[4] Raymond D., Marchany R., Brownfield M., and Midkiff . S, "Effects of denial of sleep attacks on wireless sensor network MAC protocols," to appear in IEEE Transactions on Vehicular Technology.

[5] Brownfield M., Davis N., and Fayez A., 2005. "Wireless sensor network radio power management," in OPNETWORK 2005,

[6] Ye W., Heidemann J., and Estrin D., 2004. " Medium access control with coordinated adaptive sleeping for wireless sensor networks," IEEE/ACM Transactions on Networking, vol. 12, no. 3, pp. 493–506,

[7] Raymond D., Marchany R., Brownfield M., and Midkiff S., 2006. " Effects of denial of sleep attacks on wireless sensor network MAC protocols," in Seventh Annual IEEE Systems, Man, and Cybernetics (SMC) Information Assurance Workshop, pp. 297–304,

[8] Brownfield M., Mehrjoo K., Fayez , and Davis N., 2006. " Wireless sensor network energyadaptive MAC protocol," in IEEE Consumer Communications and Networking Conference, pp. 778–782,

[9] Gouda M.G., Choi Y., and Arora A., 2004. "Antireplay protocols for sensor networks," Accessed [Online]. Available: http://www.cse.ohio-state.edu/

[10] Wood A.D. and Stankovic J. A., 2002. "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54–62,.

[11] Xu W., Trappe W., Zhang Y., and Wood T., "The feasibility of launching and detecting jamming attacks in wireless networks," in Eleventh Annual International Conference on Mobile Computing and Networking, January 1994. pp. 46–57, May 2005., National Institute of Standard and Technology,

[12] Wood A. D., Stankovic J. A., and Zhou G., "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks, " in Fourth Annual IEEE Communications Society Conference on Sensor,

Mesh, and Ad Hoc Communictions and Networks, pp. 60–69, June

[13] brownfieldM. 2005 .“wireless sensor network denial of service attack”, in sixth annual IEEE Systems,Man,Cynetics workshop ,

Manju.V.C received BE Degree from M.S university, India and M.E degree from M.K University. Currently she is doing PhD under University of Kerala, India. She has also done a short term course in Wireless Networking from Indian Institute of Science. Bangalore. Her research interest includes wireless networks .wireless sensor networks and link layerprotocols