ISSN 22773061

Defending Against Denial of Sleep Attack in Wireless Sensor Network

Manju. V.C.

Research Student, Kerala University.

Kerala University, Palayam.Trivandrum,

Pin code: 695034 Kerala. India.

Email id:manju_tvm@yahoo.com:

Phone no: 91-9886595205

Dr.Sasi Kumar.

Professor. Marian Engineering College

Marian engineering college, Menamkulam,Kazhakuttam,

Trivandrum, Pin code:695582;

Email:drmsasikumar@yahoo.com

Phone no: 91-4712599353

Abstract— A wireless sensor network is a wireless network organized with a large number of sensor nodes with specialized sensors that can monitor various physical attributes such as temperature, pressure, vibration, and sound. Sensor nodes are powered up with batteries. Due to unattended nature of the deployment, the sensor nodes' batteries cannot be recharged. In such conditions, 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 for the node, so that the lifetime of a node reduces. This problem is popularly known as Denial of sleep attack. In this paper, we propose an effective solution }to defend against such attacks in a sensor network. Our proposed solution introduces communication overhead only when the attack is suspected and also the defending mechanism is triggered only in the area of attack. Also the analysis shows that our solution is very strong against SYNC replay attack and jamming attacks.

Keywords— security; sensor networks; denial of sleep attack.

ISSN 22773061

I. INTRODUCTION

WSN (Wireless Sensor Networks) 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. 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.

The S-MAC protocol [1] uses a fixed duty cycle, with a default of 10%, during which traffic is exchanged between nodes. By placing radios in sleep mode the rest of the time, node lifetime is significantly increased. In S-MAC, sensor nodes organize themselves into virtual clusters using periodic broadcast synchronization (SYNC) messages. Upon deployment, a node listens for a SYNC message. If it does not hear one before timeout, it broadcasts a SYNC message announcing its sleep cycle. Nearby nodes overhear this message and synchronize their schedules to the sending node. SYNC messages are repeated periodically to correct time drift and keep virtual clusters sleep cycles synchronized. If a node overhears two SYNC messages, it will adapt both duty cycles to maintain network connectivity. Figure 1 shows the S-MAC frame structure. Radios in networks using this protocol will be asleep 90% of the time, thereby producing an almost 10-fold improvement in node life over MAC protocols that do not use energy-saving techniques.

T-MAC [2] improves on S-MAC by concentrating all traffic at the beginning of the duty period as depicted in Figure 2, thus trading network latency for power conservation. The arrows in the figure indicate transmitted and received messages. T-MAC uses the same SYNC mechanism to form virtual clusters as S-MAC. Instead of remaining awake for a set period, however, an adaptive timeout (TA) mechanism allows nodes to transition to sleep mode when there is no more traffic in the cluster. When a node is awake, any time it senses activity on the wireless channel; it resets its time-to-sleep (TTS) to the TA value. If no traffic is observed before the TTS expires, the node transitions to sleep mode. According to van Dam and Langendoen [2], TA is set based on the longest time that a hidden node would have to wait before hearing the beginning of a CTS response message

Attackers launch attack on the underlying MAC protocols and try to keep the node active. This problem is called a denial of sleep attack. In our research, we focus on most common MAC protocols S-MAC and T-MAC. We design a secure solution on top of these protocols to avoid nodes denial of sleep attack on these protocols.

II. LITERATURE SURVEY

In this section, we explore the features in S-MAC and T-MAC which makes them vulnerable to denial of sleep attack and the existing solution to solve it.

S-MAC uses periodic SYNC packets to prevent clock drift from desynchronizing clustered nodes' schedules if network traffic is not secured with encryption or authentication, bogus SYNC packets can be crafted with arbitrary sleep Time values.

If traffic is secured, replayed SYNC packets can also be used to mount an effective denial-of-sleep attack. Even if they are encrypted, these packets are easily identified by an attacker monitoring a network cluster by their size and timing. S-MAC SYNC packets are 10 bytes long and occur during the first few milliseconds of an S-MAC frame. WSN encryption mechanisms are careful to minimize packet overhead, thereby limiting data transmission overhead, which consumes unnecessary power. Therefore, even if all packets are encrypted, various types of packets are still identifiable because their sizes increase by a constant amount. Replaying a constant stream of back-to-back recorded SYNC packets is sufficient to keep targeted nodes awake. To maximize attack efficiency, an attacker should send SYNC packets as far apart as possible to minimize attacker awake time while still keeping targeted nodes awake. Recall that each node receiving a SYNC packet calculates its new sleep time. The receiving node's next sleep time receive another SYNC packet delaying its next sleep opportunity by the same amount and keeping the node's radio awake permanently.

Although T-MAC uses the same SYNC mechanism as S-MAC, the SYNC attack above is not effective on T-MAC because of T-MAC's adaptive timeout mechanism. Under adaptive timeout, nodes transition to sleep mode after the network has been idle for a period of time defined as TA, even if the cluster-head's transmitted sleep time indicates that it will remain awake. The adaptive timeout mechanism, although designed to improve network lifetime by increasing node sleep time, leaves it vulnerable to a simple denial-of-sleep attack. By sending a constant stream of small packets at an interval just short of the network's adaptive timeout, sensor devices on a T-MAC network will remain constantly awake.

From the attacks on S-MAC and T-MAC, we see that the vulnerability is caused because there is no way to authenticate the SYNC packet. Also the network is easily susceptible to replay attack. Our solution is based on providing strong authentication to the SYNC packets, so that denial of sleep attack is defended in the 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. Network organization
2. Selective Local authentication

The sensor network is organized in a tree structure. Between the nodes in two consequent levels authentication is enforced, so that there cannot be a jammer from outside to introduce false SYNC packets or replay SYNC packets. During the deployment stage itself, the network is organized into tree structure and the S-MAC algorithm is used to adjust the sleep time and active time from lower level nodes to the top most node sink. In addition, each parent node monitors the active time of nodes below it based on the arrival interval of SYNC, if the parent node observers some suspicious behavior, it will switch levels below it follow the authentication mode. In the authentication mode, the SYNC packet must carry an authentication token to verify the claim of the sender. SYNC packets without authentication token will be rejected. The authentication token is time varying, so that replay SYNC packets can be identified and dropped.

In our work we follow two different formats of SYNC packets, one without an authentication token, and the other with authentication token. In the normal operation when the arrival interval of SYNC is under threshold, SYNC without token is used. Only when there is threshold crossover, we can suspect a denial of sleep attack and enforce SYNC with token for authentication. This authentication mode will stay till the arrival interval falls below the threshold. Once the arrival interval falls, the network falls back to SYNC with no token.

Only when there is suspect of denial of service attack, the authentication mode is enabled. This ensures there is no overhead in our work, in the normal mode. Also authentication is enforced at level below the node suspecting the denial of service, so authentication is focused only at a certain area. This way we ensure there is no overhead on whole of network due to one attacker at certain area of network. Our solution is quick to identify the denial of service attack and stop it propagating to higher levels. Our solution is also adaptive to case of mobile attackers who move across the network and launch the attacks. Due to time varying authentication token, our approach is also secure against the replay attacks.

IV. DETAILS OF PROPOSED SECURITY MECHANISM

A. Network Organization

Organizing the node is the first step once the nodes are deployed in the network. We intend to built a tree like hierarchy and organize the nodes. Sink node is at the root of the tree. Each node must know its parent node to which it needs to send packets to reach to sink. Also the parent node must know the child node from which it can receive SYNC packets.

We propose the following network organization algorithm, which is given in Figure 3 to build the network in the way it is desired for our objective.

At the first step, the sink node broadcasts a Hello Packet with its ID. The node which receives this Hello packet which is one hop away will take ID in the Hello Packet as its parent and sends Hello Response to the ID also its broadcast a new Hello Packet with its ID. The node which receives the Hello Packet will check if it does not have a parent yet and it will add the ID in Hello packets as its parent and send Hello Response to its parent. On the arrival of Hello response, node will update its child list.

We assume there is no attack on the network during this stage of network organization. We enforce the entire node are active during the step of network organization. Once network organization is complete, the entire network is now in a tree structure with each node aware of its parent and its child node.

B. Selective Local authentication

The SYNC packet for synchronizing the active time interval is authenticated while S-MAC algorithm works.

SYNC packet must carry its self ID in the packet as the first field before the sleep time. The node receiving the SYNC packet will check it is in the child list. If it is not in the child list, the SYNC packet will be rejected. This is the first level of authentication.

If the first level of authentication succeeds, the parent node receiving the SYNC packet will check the arrival interval of SYNC from the node. To do this, each parent node maintains the arrival interval of SYNC from its child nodes in its memory. If the threshold for the arrival interval is crossed, then it may be doubted for a denial of sleep attack. Here, we cannot block the node suspected, because the attack may be also cause by external attacker who knows the behavior of node and want to disable the entire operation of network by sending packet with different ID. In our proposed solution we fall into a authentication mode. The mode is enabled by the node which detects suspicion due to threshold cross.

The node sends a SYNC AUTH packet to all child nodes to fall back to authentication mode and forces them to send authentication token in further SYNC token till it receives SYNC NO AUTH packet. The child node on receiving the SYNC AUTH can cascade it to its child nodes if it observes threshold crossover. In this way, our proposed solution is able to narrow down the area of attack and enforce authentication in that area alone.

In the authentication mode enabled region, the child nodes need to send the SYNC packet to the parent with authentication token.

In work we rely on TESLA based key generation mechanism to sign the current time of node and use it as the authentication token.

We also assume here that all nodes are time synchronized. During the deployment stage itself the TESLA keys are distributed to each node.

The node will sign the current time stamp with its current TESLA key and arrive at the authentication token. The token is sent to the parent node. The parent node will decrypt the authentication token and find the timestamp. If the time difference between the timestamp in the token and the current time stamp in the parent node is less than a difference threshold [It will be in order of around 20 milli seconds on a worst case] then the SYNC packet is considered authenticated and accepted for processing in the parent node. If the authentication fails the packet is dropped.

The advantage in our authentication method is that, the replay attack is not possible. Tesla key pool size is made relative bigger, so there is no frequent repetition of keys. Also current time stamp is used for preparing authentication, so reply is not possible.

When the node is running in authentication mode and sense the threshold is dropped, it can fall back again to normal mode. It will send the SYNC NO AUTH packet to its child nodes informing them to fall back to normal mode. This way we reduce the network overhead. The child node should cascade the SYNC NO AUTH only if its detects arrival rate drops below threshold.

C. Threshold Value for detecting suspicion

Threshold value for suspicion is an important parameter. If the value is kept high, it increases the active time of nodes causing reduction in energy of nodes. If the value is kept low, it affects the authentication mechanism to trigger frequently, which cause communication overhead indirectly increasing the energy consumption in nodes. Therefore, a balance needs to be achieved such that threshold is the optimal value in triggering the authentication mode only when there is suspicion. The threshold value can be set based on the expected number of packets from the node. This has to be done based on some thumb rule. In the current work, we set the value based on the on what rate we want to collect data from nodes.

D. Protection against denial of sleep attack

In the literature survey we explained how attacks can be launched on S-MAC and T-MAC. In the proposed solution we have provided three level of security against attacks.

- First level, in the SYNC packets, node id is sent. Node rejects the SYNC packet coming from other nodes not in the child list, thereby it not possible to generate fake SYNC and launch attack on the network without the detail of topology.
- Second level, even if a attacker having knowledge of topology, it is not possible to severely launch because the parent will shift to authentication mode and ask for the authentication token.
- Third level, even if the attackers captures the SYNC packet with authentication token and try to launch attack, the token will not pass verification because the keys are dynamic and time stamp is used in authentication token.

The only way attack can be launched is a node is compromised and sends valid SYNC packets which will pass authentication. In such case, node can be blocked if its behavior is suspicious over a period of time.

V SIMULATION ANALYSIS

Mat lab based simulation is used to evaluate the performance of this algorithm. Divided into 100m × 100m 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 SMAC, SMAC with attack and proposed secure SMAC with attack. An attack is simulated by nodes frequently sending SYNC. Attackers are uniformly distributed over the network. We have used 10 key Tesla for time stamp based authentication.

Average sleep time was found by summing up all the nodes sleep time divided by number of nodes .

We also measure the computation time taken to validate the SYNC packets. The computation time arrives only when the attack is sensed. In other cases there is no computation time.

From the graph given in Figure 4 we see that the average sleep time is decreased in case of attack. This decrease in the average sleep time reduces the life time of the network. With the proposed algorithm the average sleep time increased by blocking the attack nodes that in turn increases the network life time.

Also the computation overhead is linear with the number of nodes and the attack concentration. For the uniform attacker distribution, the computation time is plotted above in Figure 5. But in real situation, the attacker will not be uniformly distributed and the computation time will be very low. Also, the computation time is involved only when the attack is sensed in terms of fall on sleep time. Therefore, in normal operations, computation time is not present.

VI. CONCLUSION AND ENHANCEMENTS

In this paper, we have detailed our proposed defending mechanism against the denial of sleep attack. The proposed solution introduces communication overhead only when the attack is suspected and also the defending mechanism is triggered only in the area of attack. Also our solution is very strong against SYNC replay attack and jamming attacks.

In the current work, the detection of attack is made using threshold. In future we will address this area to detect attack based on other parameters. Also, instead on one threshold value applicable for all the nodes, we can selectively choose threshold value based on the data generation rate of nodes. Based on the previous history of data generation, the threshold value can be set for each node separately.

V. REFERENCES

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

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

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

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

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

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

[7] D. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, “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, June 2006.

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

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

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

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

[12] A. D. Wood, J. A. Stankovic, and G. Zhou, “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] M.brownfield “wireless sensor network denial of service attack”, in sixth annual IEEE Systems,Man,Cynetics workshop, june 2005 .

Figure 1: SMAC frame structure

Figure 2: T MAC-S MAC duty cycle

Figure 3: Network organization algorithm

Figure 4: Average sleep time vs. Number of nodes

Figure 5: computation overhead vs. Number of nodes

Table 1: Power consumption and sleep transition table