International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 4; Issue: 4; April -2015

DENIAL OF SLEEP ATTACKS ON WIRELESS SENSOR NETWORKS

Vidya M

Reva University, Bengaluru
India

Abstract: Wireless ad-hoc networks platforms are becoming exorbitant and sturdy by authorizing the pledge of extensive utilization for all things from physical health examine to military identity. These sensor networks are endangered to spiteful attack. Anyhow, the hardware clarity of these devices makes protection technique delineated for traditional networks absurd. Here mainly explores these denial-of-sleep attacks, where sensor node's power supply is directed. Attacks of this type can lessen the sensor existence and have a destructive impact on this network. This paper classifies sensor network attacks in terms of these aggressors comprehension of the medium access control (MAC) layer protocol and capability to detour attestation and encryption of these protocols. These attacks from each and every classification are usually patterned to show brunt on mainly four sensor network MAC protocols. A framework for prohibiting these attacks in sensor networks is also imported.

Keywords: Medium access control (MAC), wireless security, wireless sensor networks (WSNs).

1. INTRODUCTION

WIRELESS sensor networks (WSNs) are progressively alluring for a collective of application areas, which includes security, weather analysis, military scenarios and industrial applications. The priority issue is the challenge in designing these systems to be resilient in the aspect of myriad security threats is an important issue. One such threat is the *denial-of-sleep* attack, which is a specific type of attack which points a battery-mechanized device's power supply to drain there strained wealth. The existing network lifetime may be reduced if large percentages of network nodes are attacked. The impacts of these attacks on MAC protocols have focused mainly on denial-of-sleep, which clones the network endurance under routine traffic arrangements for a classical set of MAC protocols. To make all the nodes short and modest for economical distribution in large numbers, they generally have very limited processing capability and memory capacity.

2. SENSOR NETWORK MAC PROTOCOLS

All MAC layer protocols which are designed for WSNs use various algorithms to save battery power, e.g., by placing the radio in low-power modes when not actively sending or receiving data.

2.1 Sources of energy loss

The amount of power that can be saved largely depends on the MAC protocol's ability to overcome the radio's four primary sources of energy loss, i.e., collisions, control packet overhead, overhearing, and idle listening.

2.1.1 Collisions

Collision loss refers to the energy wasted due to packet collisions on the wireless medium. If a transmission of sufficient signal strength interferes with a data packet being sent, the data will be corrupted at the receiving end. Corrupted data can sometimes be recovered using error-correcting codes (ECCs); however, ECCs add transmission overhead, which is contrary to the goal of reducing the radio transmit time.

2.1.2 Control Packet Overhead

Depending on the MAC protocol used, control packets may have to be received by all nodes within radio range of the sender, resulting in power drain in a potentially large number of nodes. If nodes can be forced to stay awake for spurious control packets, the battery life can be greatly impacted. Examples of control packets are the *request-to-send (RTS)* and *clear-to-send (CTS)* messages used by the IEEE 802.11 protocols.

2.1.3 Overhearing

Overhearing loss refers to the energy wasted by a node having its radio in receive mode while a packet is being transmitted to another node. Most WSN MAC protocols reduce overhearing by trying to ensure that a node is only awake when there is traffic destined for it. One way to pre-vent overhearing is to ignore packets destined for other nodes after hearing an RTS/CTS exchange. After overhearing RTS and CTS, nodes set a network allocation vector (NAV) interrupt based on the message duration field in the CTS message and then go to sleep. The NAV represents the duration of the entire RTS/CTS/Data/ACK sequence. Fig. 1 depicts a typical NAV scenario.

2.1.4 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 a node can be made to listen even when there is no traffic destined for it, power is wasted.

3. CLASSES IN WSNs DENIAL OF SLEEP ATTACKS

Most research on sensor network security focuses on integrity and confidentiality. This section first introduces basic WSN security mechanisms and then reviews recent research on DoS in sensor networks.

3.1 Class 1-No Protocol Knowledge, No Ability to Penetrate Network

With no knowledge of the MAC layer protocols, attacks are limited to physical-layer jamming and unintelligent replay attacks. In an unintelligent replay attack, recorded traffic is replayed into the network, causing nodes to waste energy receiving and

processing these extra packets. If nodes in the network do not implement an anti-replay mechanism, this attack causes the replayed traffic to be forwarded through the network, consuming power at each node on the path to the destination. Undetected replay has the added benefit (to the attacker) of causing the network to resend data that could subvert the network's purpose. For example, replaying traffic in a military sensor network deployed to sense enemy movement could cause combat units to be misdirected.

3.2 Class 2—Full Protocol Knowledge, No Ability to Penetrate Network

Traffic analysis can determine which MAC protocol is being used in a sensor network. With this knowledge, an attacker could expand the attack types beyond those listed earlier to include intelligent jamming, injecting unauthenticated unicast or broadcast traffic into the network, or being more selective about replaying previous traffic. Intelligent jamming uses knowledge of link-layer protocols to reduce network throughput without relying on a constant jam signal, for ex-ample, by jamming only RTS packets. Such attacks improve over constant physical-layer jamming in that they preserve attacker energy, which can be important if attacking nodes have constraints similar to those of the target nodes. Even when attacker power consumption is not a factor, intelligent jamming might be used to make it more difficult for a network to detect an attack.

3.3 Class 3—Full Protocol Knowledge, Network Penetrated.

Attacks in this category could be devastating to a WSN. With full knowledge of the MAC protocol and the ability to send trusted traffic, an attacker can produce traffic to gain maximum possible impact from denial-of-sleep attacks. The types of attacks that could be executed against each MAC protocol. Table II classifies the types of denial-of-sleep attacks avail-able based on the attacker's protocol knowledge and ability to penetrate the network. A fourth case, i.e., no knowledge of the protocol but an ability to penetrate the network, is not considered since the ability to penetrate the network assumes full knowledge of the MAC layer protocol.

Attack Type	*Class I* *No protocol knowledge, no network penetration*	*Class II* *Full protocol knowledge, no network penetration*	*Class III* *Full protocol knowledge, network penetrated*
Constant jammer	√	√	√
Deceptive jammer	√	√	√
Random or reactive jammer	√	√	√
Intelligent jammer		√	√
Untrusted unicast/broadcast		√	√
Trusted rogue unicast/bcast			√
Unintelligent replay	√	√	√
Intelligent replay		√	√
Full domination			√

Table 1 Classification of WSN Denial of Sleep Attacks

4. EFFECTS OF DENIAL OF SLEEP ATTACKS ON SELECTED MAC PROTOCOLS

4.1 Network Model

Each network is modeled in MATLAB using similar configurations. The Mica2 models are based on the TinyOS protocol implementations available on Sourceforge.net [19]. Since none of these protocols have been implemented for CC2420-based platforms at the time of this writing, the Tmote Sky models assume the basic functionality of the protocols and are adapted to the increased data rate of the CC2420 transceiver and the specified IEEE 802.15.4 interframe spacing duration.

. 4.2 Denials-of-Sleep Attacks and Impacts

The results of each of the attacks are given in Table IV. In our models, transmit and receive pairs for all traffic are randomly assigned in a uniform distribution to equally distribute energy consumption across the nodes. We assume that all nodes are simultaneously deployed with fresh batteries and that new nodes are not added to the network during its lifetime. Network lifetime is defined as the average time between network deployment and the time that nodes' power supplies are exhausted.

4.2.1 Physical-Layer Jamming Attack

The first attack classification in Section IV considers an attacker with no protocol knowledge and no ability to penetrate the network. This classification of attack is modeled using a deceptive jamming attack, as described in , in which a constant stream of bytes is broadcast into the network. Under this attack, S-MAC is unable to transmit data and nodes remain awake during the entire 10% duty cycle because they are not able to enter NAV sleep.

4.2.2 DoS Unauthenticated Broadcast Attack

The second attack classification considers an attacker with full protocol knowledge but no ability to penetrate the network. In this case, the attacker broadcasts traffic into the network following all the MAC protocol rules for timing and collision avoidance. Under S-MAC, T-MAC, and B-MAC, these messages are received by all nodes, but are discarded because they cannot be authenticated.

4.2.3 Intelligent Replay Attack

Another attack in the category of full protocol knowledge but no network penetration is an intelligent replay attack. If an attacker can distinguish control traffic from data traffic under S-MAC, SYNC packets can be replayed at an interval short of the sensor cluster's duty cycle, effectively restarting the duty cycle and pushing back the sleep period each time. This would keep all nodes awake until they run out of power. In G-MAC, FRTS messages should be replayed such that the corresponding NAV periods fill the contention-free portion of each frame. For a message size of 64 B, 75 FRTSs would fill the contention-free period, ensuring that at least one node is awake at all times. This effect, combined with a longer GTIM message that all nodes must receive, results in a network lifetime of 160 days, assuming all the FRTSs are for unicast packets. If any of the replayed FRTS messages happen to be broadcast FRTSs, the network lifetime is further degraded because all nodes must wake up during the contention-free period to listen for the broadcasts.

4.2.4 Full Domination Attack

The final attack classification is one in which an attacker has full protocol knowledge and has penetrated the network. This type of attack might be mounted using one or more compromised nodes in the network. Once this level of network penetration is achieved, all of the MAC protocols are susceptible to worst-case power consumption. An attack against S-MAC is simply to send a SYNC message at a frequency just short of the duty cycle to keep delaying the transition to sleep mode. The T-MAC network lifetime is minimized by continually sending packets at an interval slightly shorter than the adaptive timeout (TA) so that none of the nodes can ever transition to sleep. Although not efficient for the attacker, a deceptive jamming attack is the most effective attack against B-MAC.

5. CONCLUSION

Most current research in WSN security focuses on data confidentiality and integrity, largely ignoring availability. With-out the ability to secure the physical medium over which communication takes place, sensor networks are susceptible to an array of potential attacks focused on rapidly draining sensor node batteries, thereby rendering the network unusable. The primary contribution is it classifies denial-of-sleep attacks on WSN MAC protocols based on an attacker's knowledge of the MAC protocol and ability to penetrate the network.

6. REFERENCES

[1] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in Proc. 6th Annu. IEEE SMC Inf. Assurance Workshop, Jun. 2005, pp. 356–364.

[2] Tmote Sky Datasheet: Low Power Wireless Sensor Module, Moteiv Cor-poration, Redwood City, CA. Accessed Feb., 2006. [Online]. Available: http://www.moteiv.com/

[3] *Mica2 Datasheet*, CrossBow Corporation, San Jose, CA. Accessed May 2006. [Online]. Available: http://www.xbow.com/

[4] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordi-nated adaptive sleeping for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 12, no. 3, pp. 493–506, Jun. 2004.

[5] T. VanDam and K. Langendoen, "An adaptive energy-efficient MAC pro-tocol for wireless sensor networks," in Proc. 1st ACM Int. Conf. Embed-ded Netw. Sensor Syst., Nov. 2003, pp. 171–180.

International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241
Volume: 4; Issue: 4; April -2015

Vidya M

Reva University, Bengaluru
India

Manuscript Received on 13/3/2015

Acceptance Notification : 05/05/2015

Publication of Manuscript : 12/05/2015