Denial of Service Attacks in Wireless Sensor Networks

[1]Vidya M, [2]Reshmi S

M.Tech Student, Assistant Professor
Visvesvaraya Technological University, India
Email: [1]Vidya.M1389@gmail.com, [2]Reshmi101@gmail.com

Abstract- Network survivability is the capacity of a network keeping connected under loss and intrusions, which is a major concern to the design and design interpretation of wireless ad hoc sensor networks. Ad-hoc low power wireless networks are in inquisition in both discerning and ubiquitous computing. The proposed method discusses about energy draining attacks at the routing protocol layer, which drains battery power. An innovative approach for routing protocols, affect from attack even those devised to be protected which is short of protection from these attacks, which we call energy debilitating attacks, which enduringly disable networks by quickly draining nodes battery power. These energy depletion attacks are not protocol specific but are disturbing and hard to notice, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. 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 -Denial of service, security, routing, ad hoc networks, sensor networks, wireless networks, Medium access control (MAC), wireless security, wireless sensor networks (WSNs).

I. INTRODUCTION

AD hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as continuous connectivity, ubiquitous on-demand computing power and deployable communication required instantly for first responders and military purposes. These networks already monitor factory performance, environmental conditions to name a few applications [1]. Due to their organization, these networks are particularly vulnerable to denial of service (DoS) attacks research work has been done to enhance survivability. Here, we consider how routing protocols though designed to be secure, lack protection from these vampire attacks which deplete life from these networks. There are three primary contributions in the paper. First, we evaluate the vulnerabilities of existing protocols thoroughly to routing layer battery depletion attacks. Second we observe that security measures to prevent these depletion attacks are orthogonal to those which are used to protect existing secure routing protocols, and its infrastructure [1]. 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. These wireless sensor networks (Fig 1) offer certain enhancements and capabilities to assist in the national effort to increase alertness to potential terrorist threats as well as operational efficiency in civilian applications. Wireless ad hoc sensor networks are classifies mainly two types whether the data in the network is aggregated and whether or not the nodes are individually addressable.

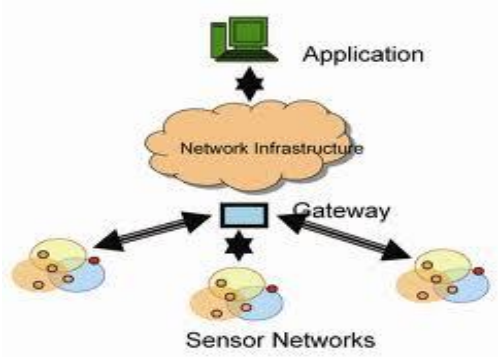

Fig 1: Wireless Sensor Networks (WSNs)

II. OVERVIEW

The immoderate resource limitations of sensor devices constitute substantial provocation to resource-aching certainty systems. The hardware curtailment entails immensely coherent security algorithms in terms of memory, bandwidth, and computation complexity. This is no superficial endeavor. Energy is the most valuable expedient for sensor networks. In terms of power communication is very expensive. In order to be energy efficient a special effort should be given to security mechanisms to make it communication efficient. A significant challenge for security mechanisms is posed for sensor networks. Simply networking from tens to thousands of nodes has proven to be a substantial task. Providing security to these networks is equally in demand. Security mechanisms must be ascendable to very large networks to sustain communication efficiency in networks.

Depending on the functions of these sensor networks, the sensor nodes may be left untended for lengthy duration of time.

Sensor Network Mac Protocol

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.

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.

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.

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.

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.

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.

III. 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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

V. ATTACKS FOCUSED ON WIRELESS AD-HOC SENSOR NETWORKS

Here we mainly focus on these attacks which are two types that are used for Denial of Service Communication.

Carousel Attack

In this carousel attack (Fig 2), a malicious node sends a packet with a composed route which as a series of loops, so that the same node would appear in the route for many times [1]. This strategy is mainly used to increase the length of the route which is beyond the total number of nodes in the existing network, only limited by the number of entries which is allowed in the source route [5]. Example for this type of route is given in Fig.2 the thin shows the malicious path and thick path shows the honest path.

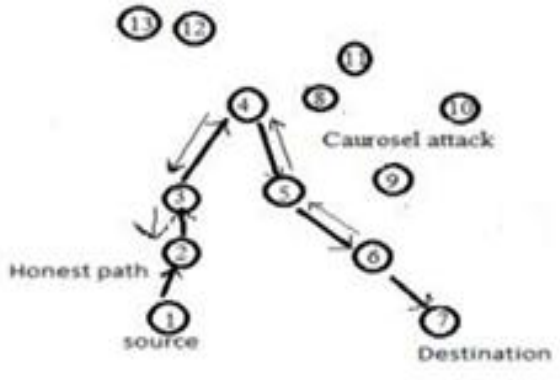

Fig 2: Shows the carousel attack same node appears in the route many times.

Stretch Attack

Another such attack in the same way is the stretch attack, where a malicious node in network constructs artificially long routes from source, which cause packets to traverse larger than optimal number of nodes [5]. In the example given below (Fig.3) honest path is shown with thick lines and adversary or malicious path with thin lines. Thus malicious path take a long distant then the honest path by making more consumption of energy.

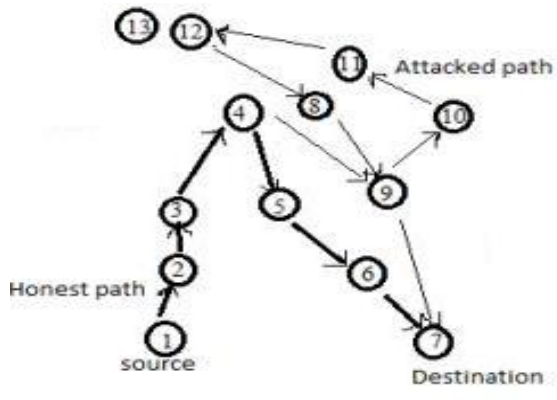

Fig 3: Shows the stretch attack where malicious path chooses longest route.

In contrast to other attacks this attack shows more uniform energy consumption for all the nodes in the existing network, as it increase the length of the route, by causing more number of nodes to process the packet in the network. While vampire attacks make network-wide energy usage significantly as individual nodes are also affected noticeably till destination. Thus long routes will lose almost 10 percent of their total energy reserve per message.

VI. PROTOCOLS ANDASSUMPTIONS

Here in this section we mainly discuss various protocols proposed by various researchers in wireless sensor networks. Here attacks have not rigorously defined at routing layer. Thus power depletion can be found in, as "sleep privation affliction". As we explained, the proposed attack prevents nodes from entering a sleep cycle, and which leads to faster depletion of batteries.

Stateful Protocol and their attacks

In this protocol is where nodes are aware of their forwarding decisions, topology and its state. Here servers are supposed to recall so that it can be resumed. State and distance vector are two important classes of stateful protocols. OLSR and DSDV are examples of link-state and distance-vector. Both of these protocols are aggressive, which directs to all available nodes in the network and by decreasing the initial delay. Each node maintains a routing table which contains all accessible destinations and number of hops and next node to reach the destination and systematically send table to all of its neighbors so that it can update topology. There are mainly two types of attack they are directional antenna attack and malicious discovery attack. In this first attack the malicious have little control over the progress of packets, but they still waste their energy by restarting a packet in various parts of network. Second attack is also called as spurious rote discovery. This type of attack becomes serious when nodes claim lengthy routes have changed.

Stateless Protocol and their Attacks

This protocol does not require the server to retain session information about each communications partner for the duration of multiple requests and its only communication protocol which treats each and every request as an independent transaction which is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.

Clean state secure routing protocol

The PLGP protocol is modified as clean state secure routing protocol which can resist these attacks during the forwarding phase. This protocol was accessible to these attacks even though they were said to be secured. PLGP consists of a topology discovery phase, which is

followed by a packet forwarding phase, which has former optionally repeated on a fixed schedule to ensure that topology information stays current.

VII. RELATED WORK

Existing research work on secure routing protocols attempts to ensure that malicious nodes cannot cause path discovery to return an invalid network path as these nodes do not alter discovered paths but, by using existing valid paths in the network and protocol compliant messages. These adversaries mainly have limited power to affect forwarding of packets in network, making these protocols resistant to these vampire attacks. By the use of directional antenna they can consume more energy by restarting packet in various parts of the network. Other such attack is spurious route discovery where each node will forward route discovery packets which means by sending a message it is possible to cause flood attack in network.

Drawbacks of existing system

1. Adversaries have limited power.

2. Security level is low.

3. Lost productivity.

4. Various DOS attacks.

5. Spurious route discovery.

VIII. PROPOSED SYSTEM

Nodes mainly identify by their neighbors by considering the most significant bit and they construct a tree by considering all relationships among neighbors and finally it forms a group which will be used for routing and addressing. It mainly uses No-backtracking property which it is satisfied by a given packet if and only if it makes progress towards destination in the existing network space.

Advantages of the proposed system

1. Highly secured authentication.
2. High efficiency.
3. Timely delivery of packets.
4. No flooding.

IX. RESULT ANALYSIS

Topology and cluster head detection

The topology we have used here is a mesh topology. In this case each and every node sends a message to the other nodes which is detected in the network. Nodes maintain a record once it detects the node and this is done by using multicast socket. Based on range, battery power and mobility cluster power is detected.

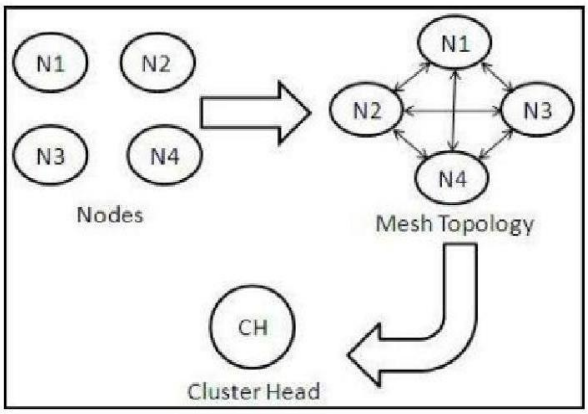

Fig 4: Topology and cluster Head Detection.

Tree formation and Route Discovery

Trees are formed as nodes form group. Each node starts with group size 1 and virtual address 0 so that one group is formed. Similarly other groups are also formed. When two nodes form a group their group size becomes 2 with one node taking a virtual address 0 and other taking the address 1.Each group can have their own group address. Example: node 0 in one group0 becomes 0.0 and node 0 in group 1 becomes 1.0. Each time a group is added or merged the address of each node is lengthened by one bit . Thus a tree structure is formed with address in the network and node address as leaves. Generally small groups form with 1 node later they merge to form large groups.

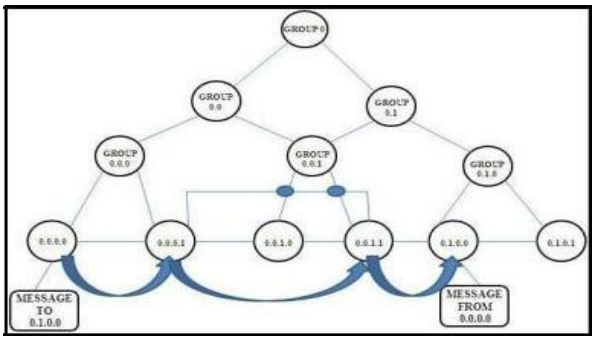

Fig 5: Group Identification.

Packet Forwarding

This module is used to transmit packet to nodes using the above formed tree structure (Fig.6). Here each node has independent route constructed from the tree structure and it also checks for the condition to match No Backtracking property or else it leads to an attack. During this phase, each node is independently of taking decisions. Each node determines the next hop by finding the most significant bit of its address that differs from the message originator's address while receiving a packet. Thus every forwarding event shortens the logical distance to the destination, since every node addresses which is chosen should be surely adjacent to the destination. The function used for forwarding of packets is as follows:

```
1.  Function forward_ packet ()
2.  s←extract_ source _ address (p);
3.  c←closest _next _node(s);
4.  If is _neighbor then forward(p ,c);
5.  Else
6.  r←next _ hop _to _non _neighbor (c);
7.  forward (p ,r);
```

X. CONCLUSION

In this paper we mainly talk about energy debilitating attacks, a new class of resource exhaustion attacks that use routing protocols to permanently disable these networks by depleting nodes battery power in existing network. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols. We also saw how to overcome these attacks by increasing the energy of the node in the network.. We defined about PLGP routing protocol that constrains damage from these attacks by validation the packets in each and every node by choosing shortest routes in the network. 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.

XI. REFERENCES

[1] Eugene.Y.Vasserman, Nicholas Hopper, Vampire attacks Draining life from adhoc wireless sensor networks, IEEE volume 2 (2014).

[2] Maximum lifetime routing in wireless networks, IEEE/ACM Transactions on Networking 12 (2004), no.4

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

[4] The network simulator — ns-2. http://www.isi.edu/nsnam/ns/.

[5] Thomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.

[6] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.

[7] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.

[8] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography, Vol. 265, Cambridge University Press, 1999.

[9] Joppe W. Bos, Dag Arne Osvik, and Deion Stefan, Fast implementations of AES on various platforms, 2009.

[10] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.

◈◈◈