NONACK In Wireless Ad Hoc Network

Trisha Mittal
Department of Computer Engineering
Netaji Subhas Institute of Technology, University of Delhi
New Delhi, India
trisha.nsit@yahoo.com

Bijendra Kumar
Department of Computer Engineering
Netaji Subhas Institute of Technology, University of Delhi
New Delhi, India
bizender@hotmail.com

***Abstract*—A wireless ad hoc sensor network (WSN) is made up of a number of geographically spread apart sensors each with a reasonable amount of signal processing and data networking ability coupled with wireless communication. One of the major challenges wireless sensor networks face today is security. Denial of service (DoS) attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. This paper explores resource depletion attack in a cooperative manner and increasing traffic on the routing layer protocol. The ease of carrying out a NONACK (Noose Noose attack) and the difficulty in its detection makes all examined protocols very susceptible to it. The worst case scenarios can see an upsurge in the network-wide usage by a factor of $O(N^2)$, N being the number of network nodes.**

Keywords— wireless ad hoc sensor network(WSN); Denial of service; attack; NONACK

I. Introduction

The WSN is built of "nodes" from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors[1].For WSNs become more and more crucial to the everyday functioning of people and organizations like military, wireless traffic, wireless surveillance, wireless parking lot, thus, availability faults become less tolerable. Wireless ad hoc networks are particularly vulnerable to denial of service (DoS) attacks and many researches have been done to enhance survivability. Attacks can be categorized in two ways: active attacks and passive attacks. Attacks that try to alter the functioning of the resources of the system are termed as active attacks and those that only analyze the system's information but do not affect the functioning of its resources are termed as passive attacks. [2]. Modification, fabrication and jamming are some of the common DOS attacks which are active attacks. Resource depletion attack is also a DOS attack which depletes the nodes batteries. In this paper we will discuss how routing protocols, even those designed to be secure, lack protection from NONACK, since they drain the life from networks nodes and also increase the delay. NONACK works in a cooperative manner provided none of the two malicious nodes being active at a time and hence they are really tough to be detected.

II. Related Work

Many resource depletion and DOS attacks have been defined, evaluated, or mitigated on various layers. With the rapid growth of Implantable Medical Devices (IMDs), their security becomes a critical issue since the attacks on the devices may directly harm the patient. Typical IMDs have restricted resources in terms of energy, processing capability, and storage. The Resource Depletion (RD) attacks are able to quickly deplete the resources of an IMD, such as battery power, thus, RD attacks can reduce the lifetime of an IMD from several years to a few weeks [3].Among various security threats, those attacks which lead to random drainage of the energy level of sensors, immensely affect the low power sensor nodes, thus, leading to death of the nodes. One of the most dangerous types of attack is sleep deprivation, where the intruder targets to maximize the power consumption of sensor nodes; so that their lifetime is minimized [4]. Another way of reducing the sensor lifetime is by targeting the sensor node's power supply as done by denial-of-sleep attack. These attacks are capable of diminishing the sensor's lifetime from years to days [5]. A framework has been proposed in the paper for defending against denial-of-sleep attack and specific techniques have been provided that can counter each denial-of-sleep susceptibility.

One of the DOS attacks is Vampire attack which involves depletion of the life of a node that is part of the wireless network [11]. This paper delves into the topic of resource depletion attacks at the routing protocol layer which permanently immobilize a network by exhausting the battery power of the nodes. A malicious packet source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes that forward the packet based on the included source route. Vampire attacks are not protocol-specific. These depend upon the characteristics of many popular classes of routing protocols. NONACK also introduce loops in the route resulting in DOS attack and resource depletion attack. NONACK is even harder to detect and cause much more delay while consuming the battery power of nodes.

III. NONACK

A. Description of NONACK

The goal of Denial of Service (DoS) attacks is to prevent availability of network services from their legitimate users [6] [7]. Its basic aim is prevention of authorized access to the resources or time delaying. DoS attack has different scenarios. First attack scenario targets the memory, storage space, or CPU of the service provider. Second attack scenario targets energy resources like the battery power of the service provider. The third scenario targets bandwidth. NONACK attack targets the second scenario. All routing protocols employ at least one topology discovery period, since ad hoc deployment implies no prior position knowledge. Limiting ourselves to immutable but dynamically organized topologies, as in most wireless sensor networks, we further differentiate on-demand routing protocols, in which topology discovery is done at transmission time, and static protocols, in which topology discovery is done at initial setup phase, where topology change is handled by periodic rediscovery. We would be focusing on on-demand routing protocol as for now.

In our attack, adversaries force the packet to create routing loops before reaching to destination and the two adversaries work in a cooperative manner. We call it NONACK as shown in Fig. 1.

When one of the adversaries is performing NONACK, the other partner (adversary) will be behaving just as an honest node and we call it as its resting stage. First adversary will initiate the second one to create loops before going into rest mode and in this manner second adversary will again initiate first one before going to rest. In this way one of the two adversaries will be working whole the time provided the same node never work maliciously for the whole time and also the two will never behave malicious at the same time. Hence it becomes really very difficult to detect NONACK attack. The limited verification of message headers at forwarding nodes becomes the Achilles heel for the source routing protocol. During a NONACK a single packet is made to repeatedly traverse the same set of nodes until delivery to the destination. This will consume the battery life of all the nodes in the network.

The algorithm for the NONACK is given in Fig. 2.

B. Assumptions

We assume that only adversaries originated messages may have maliciously composed routes. Our adversaries are malicious insiders and the level of resource and network access is same as done by an honest node. Once the battery power is exhausted, the node will be permanently disabled. Initial energy level of network is 200 joules. We assume all the nodes have the same initial transmission range of 250 meters, traffic type is 512 bytes cbr, size of simulation area 1500*1500.

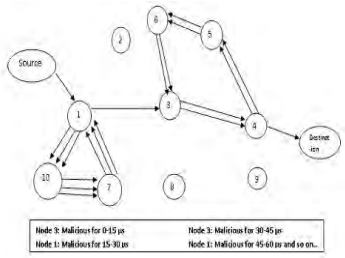

Fig. 1. NONACK

```
N<-node list;
s<- source_address;
d<- destination_address;
flag<-0;
select x<- routing protocol;
call route_discovery(s,d);
return posible_path_list;
executed_path=best_path(possible_path_list);
m1=pick_Malicious(executed_path_node_list) //choose a node m1 in executed path as malicious node
loop1=formloop(m1,(N-executed_path));
m2=pick_Malicious(executed_path_node_list- m1);
loop2=formloop(m2,(N-executed_path));
for(count=1;count<1000000;count+2) //total simulation time is 15 second and loop switches after every 15 microsec
{
if(flag==0)
        {
        executed_path=executed_path + loop1;
        delay(15) //(delay(time in microseconds))
        flag=1;
        executed_path=executed_path - loop1;
        }
        if(flag==1)
        {
        executed_path=executed_path + loop2;
        delay(15)
        flag=0;
        executed_path=executed_path - loop2
        }
}
```

Fig. 2. Algorithm of NONACK

IV. SIMULTION OF NONACK

We evaluated NONACK in a randomly generated 30 to 50 sensor node topology and DSR(Dynamic Source Routing) routing protocol and two randomly selected malicious DSR agents, using the ns-2 network simulator [8]. Mac 802.11 and Omni antenna is used for data communication and covering the transmission range. The routing is performed between sensor nodes, let the data packets be 512 bytes and the initial energy level of nodes be 100 joules. The graphical constraints like throughput, packet delivery ratio, delay are used to evaluate the performance of network.

A. DSR

DSR is a reactive routing protocol which does not use periodic table-update messages as done by table-driven routing protocols [9]. DSR, specifically designed for use in multi-hop wireless ad hoc networks, allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration.

For restricting the bandwidth, the process to find a path is only executed when a path is required by a node (On-Demand-Routing). In DSR the sender (source, initiator) determines the whole path from the source to the destination node (Source-Routing) and deposits the addresses of the intermediate nodes of the route in the packets. Compared to other reactive routing protocols like Adhoc On Demand Distance Vector routing[10] and DSDV, DSR is beacon-less which means that there are no hello-messages used between the nodes to notify their neighbors about her presence.

DSR is based on the Link-State-Algorithms which mean that each node is capable of saving the best way to a destination. Also if a change appears in the network topology, then the whole network will get this information by flooding.

B. Path Selection And Loop Formation

In this case, Node–20 acts as source node and 45 acts as destination node, source node broadcast a RREQ message to reach destination, and destination replies RREP message to source through three paths,

- Priority path_1: 45-24-23-22-21-20
- Priority path_2: 45-46-30-29-28-27-26-20
- Priority path_3: 46-44-18-17-16-15-14-20

Source node selects the first priority path, since it has the minimum hop count and nearer distance. And source node 20 transmits data to destination through intermediate nodes 21-22-23-24, at certain time intermediate node 24 behave as a malicious node and forms a loop, in loop node 18-17-16-10-11-12-18 will be involved as shown in Fig. 3, then the packet is transmitted to destination, in addition another intermediate node 22 also forms a loop with nodes-28-34-35-29-28, and then the packets are transmitted to destination. Both the malicious node 24 and 22 forms a loop alternatively with the time interval of 15 micro sec, hence make energy consumption much larger, and affect the network performance.

V. Results and Comparison

NONACK is a more powerful and cooperative version of carousel attack mentioned in vampire attack [8]. In carousel basically only a single node make the loop but in NONACK two nodes perform this in cooperative manner and hence resulting in more damage in terms of delay, throughput and packet delivery ratio and even much different to find that exact which node is malicious.

A. Packet Delivery Fraction (PDF)

This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes throughout the simulation.

$$PDF = \frac{\text{Number of received packets}}{\text{Number of sent packets}}$$

The packet delivery ratio of the network in presence of NONACK is 79% and in presence of carousel is 94% as shown in Fig. 4.

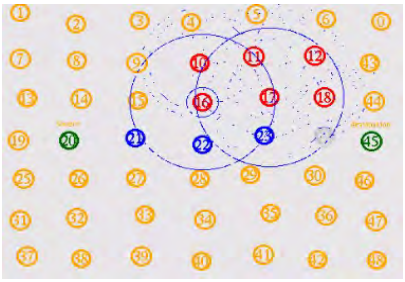

Fig. 3. Simulation of NONACK

B. Average End-to-End Delay (AED):

The packet End-to-End delay is the average time that a packet takes to traverse the network. This is the time from the generation of the packet in the sender up to its reception at the destination's application layer and it is measured in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges.

$$AED = \frac{\Sigma\,(\text{time received} - \text{time sent})}{\text{Total data packets received}}$$

The delay time is determined in presence of NONACK is 22 seconds and in presence of carousel is about 10 seconds as shown in Fig. 5.

C. Throughput

Total number of Bytes successfully transmitted from source to destination per second. It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet.

The throughput rate in presence of NONACK is 60 kb/s and in presence of carousel attack is 80 kb/s destination as shown in Fig. 6.

D. Packet loss

Packet loss is the failure of one or more transmitted packets to arrive at their destination.

The packet loss determined as in presence of NONACK is 26 and in presence of carousel is 18 as shown in Fig. 7.

E. Energy consumption

Energy required for transmitting a packet from source to destination.

The energy consumption of NONACK is 85 joules and for carousel attack is 65 joules as shown in Fig. 8.

The energy consumption in normal data transfer, in presence of NONACK and in case of carousel attack is shown in Fig. 9.

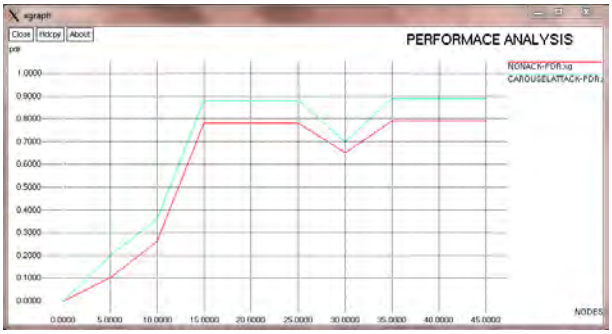

Fig. 4. PDR simulation results for NONACK and carousel attack

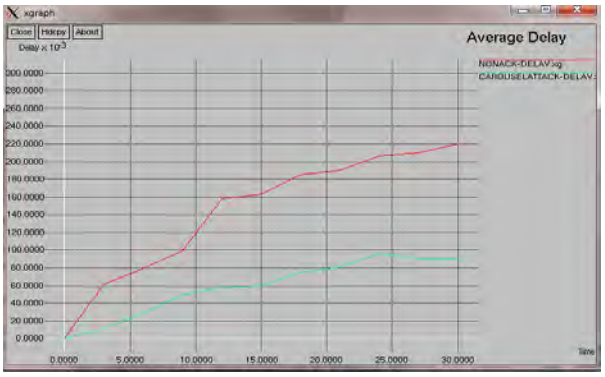

Fig. 5. AED simulation results for NONACK and carousel attack

Fig. 6. Throughput simulation results for NONACK and carousel attack

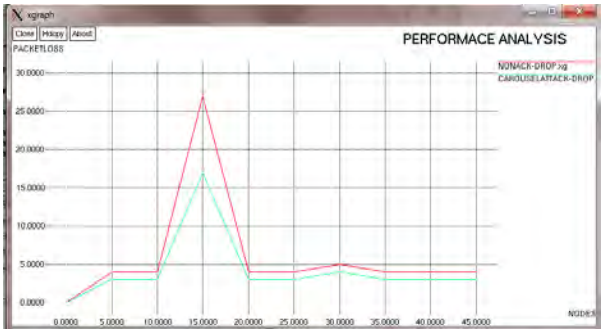

Fig. 7. Packet loss simulation results for NONACK and carousel attack

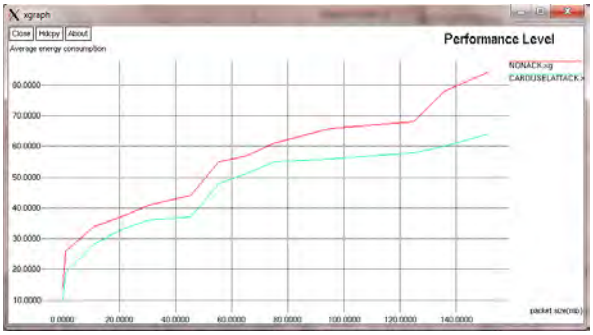

Fig. 8. Average energy consumption in presence of NONACK and carousel attack.

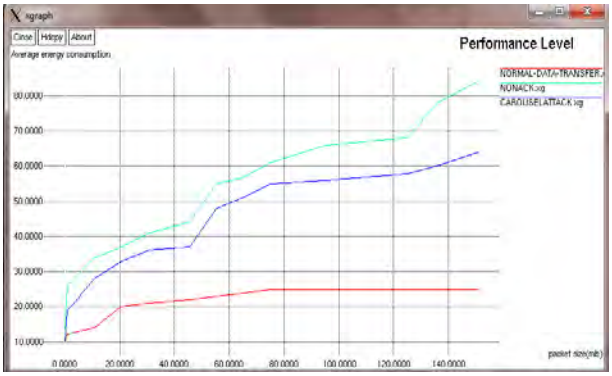

Fig. 9. Average energy consumption in case of normal data transfer and in presence of NONACK and carousel attack.

VI. CONCLUSION

In this paper, we have defined NONACK as a resource consumption attack that disables ad hoc wireless sensor networks by exhausting the battery power of the member nodes by using the routing protocol. This also results in delivery delay as the packet first revolves in loop before going to destination. Simulation results show that NONACK results

in almost double end-to-end delay in comparison with carousel attack of vampire. Also it results in higher energy consumption and low throughput.

We will try to give a solution for this attack as the future work.

References

[1] Eiko Yoneki, Jean Bacon, "A survey of Wireless Sensor Network technologies: research trends and middleware's role", University of Cambridge Computer Laboratory,Cambridge CB3 0FD, United Kingdom, September 2005.

[2] "What is Active Attack?" available at http://en.wikipedia.org/wiki/Attack_%28computing%29.

[3] Xiali Hei, Xiaojiang Du," The Resource Depletion Attack and Defense Scheme", SpringerBriefs in Computer Science 2013, pp 9-18

[4] Tapalina Bhattasali ,Rituparna Chaki ,Sugata Sanyal "Sleep Deprivation Attack Detection in Wireless Sensor Network", International Journal of Computer Applications (0975 – 8887),Volume 40– No.15, February 2012

[5] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols,"IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[6] Kemal Bicakci,Bulent Talavi,"Denial-of-Service attacks and countermeasures in IEEE wireless networks,"Computer Standards & Interfaces 31 (2009) 931-941

[7] Imad Aad,Jean-Pierre Haubaux,Edward W.Knightly, "Impact of Denial of service attacks on Ad Hoc Networks ".

[8] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012.

[9] David B. Johnson, David A. Maltz, Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks" http://www.monarch.cs.cmu.edu/

[10] "Mobile Ad hoc Networking (MANET) with AODV", available at http://www.cs.virginia.edu/~jwang/STIL_files/NovaRoam_documents/AODV%20White%20Paper.pdf

[11] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", Published by the IEEE CS, CASS, ComSoc, IES, & SPS, 2013.

.