Power Consumption Attacks on Wireless Sensor Networks

Micah Thornton, Robert Santoski, Ryan Sligh
{mathornton, rsantoski, rsligh}@smu.edu

***Abstract*—As the name plainly states, wireless sensor networks (WSNs) are not connected by wires to anything: including a power supply. These devices often make use of cheaper disposable and replenishable power supplies such as batteries. The strength of the battery used determines how long each of the independent wireless sensor nodes will be able to opperate without supply replacement. The nature of these limited power supplies opens up nodes of WSNs to attacks that drain the limited power supply of the node in order to cause the node to halt a selected operating procedure. In this paper we simulate a power consumption attack on a node of a WSN in order to help devise, and possibly validate certain mitigation strategies for power consumption attacks on these nodes.**

CONTENTS

I Introduction 1
- I-A Previous Work 1
- I-B Contents 2
- I-C Goal 2

II Methodology 2
- II-A Adversarial Assumptions . . 2
- II-B Target Assumptions 2
- II-C Simulation Setup 2

III Results and Analysis 3
- III-A Simulation Details and Result gathering 3
- III-B Analysis 4

IV Conclusion 5
- IV-A Future Work 5
- IV-B Remarks 5
- IV-C Limitations 5

References 5

I. INTRODUCTION

A. Previous Work

Wireless Sensor Networks(WSN) are being used in a variety of exciting applications. The UUTE project[1] will provide more independence and mobility to the elderly and recovering patients by using wearable wireless sensors to monitor their health. But many WSN applications depend on a limited battery as a source of energy. Using power effectively is important in keeping the WSN functional and cost efficient. In[2],Manju identifies the activities which waste battery power the most in a WSN node. A node wastes energy when the packet it sends becomes corrupt due to a collision, and retransmissions are required since error correcting codes, which use additional power, are not often used [3]. Also, overheating is when a node is needlessly awakened from sleep mode when it intercepts a transmission that was meant for a different node. Misuse of control packet [2] can also drain power by keeping a node listening, until a timeout occurs, for packets that will never arrive or by causing the a node to needlessly transmit responses.

An attacker could take advantage of these power wasting scenarios and force them to happen more often than they normal would. Any attacks that causes these effects for long periods of time are considered Denial-of-Sleep [3] attacks because a node is being forced to use up power to performing meaningless tasks instead of switching to a power-conserving sleep mode. These previously mentioned battery draining scenarios all occur in the MAC layer, but Vasserman and Hopper[4] bring up the point that attackers could achieve the same goal in the network layer by forcing the packets to take the longest path possible to reach its destination, or worse: route the packets in an endless loop, which is called a carousel attack. Vasserman also explains that attacker nodes on a wireless ad-hoc network, such as a WSN, typically try to use as few transmissions as possible while maximizing the wasted power consumption of victim nodes. Instead of blasting control packets at a high rate, attacker nodes smartly send transmission to avoid being

identified as malicious by nearby nodes.

B. Contents

In this paper, we will be simulating several simple wireless sensor node attacks in order to figure out methods of protecting against such attacks. First we will establish what resources and what information the attacker will have for each simulation. Then we will explain the details of the scenario we are simulating, including the type and the size of battery used by the node, and the size of the packets that will be transmitted. We will also describe how the simulation is set up, as well as the assumptions we took while designing them. With the framework of the simulation established, we will analyze the patterns and implications of the collected data. Then we will use the data analysis to support our proposal for countermeasures against power consumption attacks.

C. Goal

The goal of this simulation is to gain an understanding of the effects of power consumption attacks on WSN nodes. We will be able to understand the weaknesses and limitations the sensor nodes, and we can use this insight to figure out mitigation techniques that could potentially be put into practice. Also we want to be able to recommend certain design choices, such as battery type, when manufacturing WSN nodes.

II. Methodology

A. Adversarial Assumptions

There are a few assumptions that are made about the supposed attacker in the simulation scenario. The first assumption is that the attacker is connected wirelessly to the target node. Another assumption is that the attacker has knowledge about the node they are attacking. The attackers goal in this scenario is to consume enough of the power from the target node so that the node is no longer able to transmit packages. Another assumption is that the attacker has the capabilities to send a high volume of packets very quickly to the target node.

B. Target Assumptions

The target node similarly has assumptions associated with it in the simulation. We assume that the node is a wireless sensor node connected to other wireless sensor nodes. We also assume that the most power in the node is allocated to transmission, with reception being second. We assume that the target node has limited power to allocate to each of its functions.

C. Simulation Setup

We are using NS3 to simulate two wireless nodes connected to each other. We are simulating two different kinds of attacks on the target node. The first attack is one in which many packets are sent rapidly from the attacker node to the target node in order to force the target node to accept a multitude of transmissions and drain its battery as shown in the figure below.

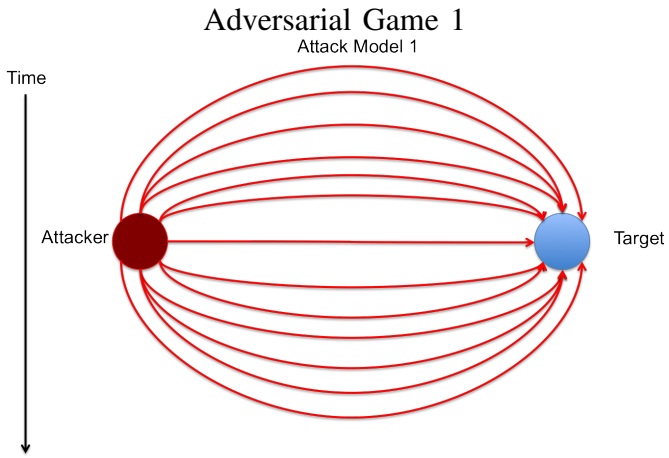


Fig. 1. The figure above depicts an attacker continually bombarding a node with packets which force the target node to do calculations and thereyby conttributes to the draining of the initial energy supply.

The second attack is one in which the attacker node requests a transmission from the target node but then does not send any acknowledgements. This attack forces the target node to use power trying to send (many times) a succesful transmission but never is able. This results in the target node slowly being drained of power while transmitting it is diagramed below.

For the purpose of simplicity and to limit variables we are modeling two nodes, an attacker and a target, as opposed to a large network of nodes. When setting up the model we have multiple variables that we concern ourselves with that can affect

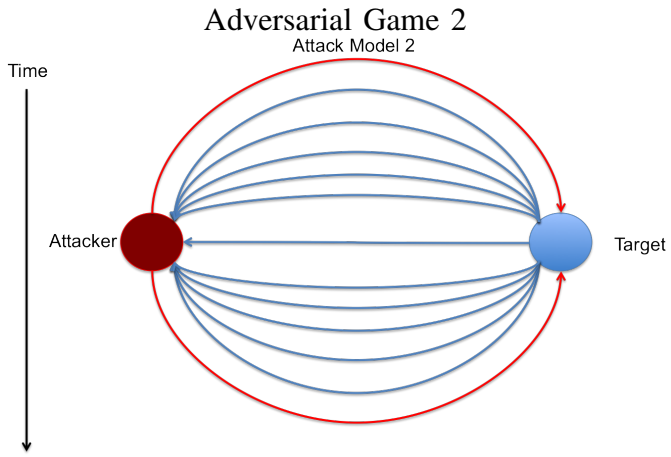


Fig. 2. The figure above depicts an attacker requesting a transmission from a node with forces the target node to send the message over and over (because the attacker doesn't send an acknowledgement for a long time) conttributes to the draining of the initial energy supply.

the simulation. The most important variables are the battery size of the target node, the number of packets being sent from the attacker to the target, and the time interval at which the attacker sends the packets. Other variables include distance between the two nodes and the size of each packet. The simulation creates two nodes that are both assigned an ipv4 address and connects them together via WiFi. The simulation then runs the specified attack with the variables that it were assigned. While packets are being transferred the simulation prints out data after each successful transmission. The data printed is the amount of battery left before and after the packet is sent and received and the time stamp at which the packet was transmitted by the attacker node and received by the target node. The simulation ends when the target node no longer has enough power to receive packets.

III. Results and Analysis

A. Simulation Details and Result gathering

It is worth reiterating over and over again that the key premise investigated in this project up to this point is the simply energy consumption attack on a specific node that uses the wifi radio protocols. As of yet we have not adapted our model to make use of the existing WSN protocols such as LEACH, ZIGBEE, or other WPAN protocols [5][6]. Because of the limited nature of the NS3 simulation tool that has been used to simulate the power consumption attack, we are looking at problems with adapting any type of IEEE WPAN protocol, and are considering the use of a different simulation tool in our future efforts.

Several factors were investigated by the initial simulation of a Power Consumption attack on WiFi radio (WiFi radios are used in the simulation in order to estimate Tx Current and Rx Current and because they are similar to WSN communications). As mentioned in the set up section of our methodology, we used an attack that caused the target node to receive a lot of communication in a short amount of time (1 packet/ 10 ms). The primary advantage of our simulation is that we can manipulate the initial energy supply of the target node. We simulate the initial energy supply based on a few factors, first: what is the internal acid of the battery, second: what is the weight of the battery, third: the potential difference of the battery is assumed to be a constant 3.6 Volts. the information used in these calculations was taken from [7].

We ran the simulation multiple times varying the size of the packet transmitted, and the parameters of the initial energy source. The results of the simulation were not extremely surprising, but necessary to begin an analysis of attacks on WSN nodes. It is also worth noting before we proceed that the packet sizes were varied in powers of two (as they likely would be).

The network simulation was done in NS3, and was based on an example entitled "energy-power-model.cc" included in the standard distribution. We do not take credit for the full simulation, but instead would like to thank the authors of the original code that we modified, Sidharth Nabar and He Wu. The main modification to the original example included an increase in the rate of the number of packets transmitted from 1 every 10 seconds to 1 every 10 milliseconds. In our methodology section we explain that the attacker is assumed to have unlimited transmission capabilities, thus this increase in speed is justified. Another modification was made by allowing the initial energy of the power supply (in Joules) to be called from the command line. This modification allowed for easy iterative manipulation of the essential arguments for our research.

In addition we wrote a script that, given the weight and acid-type of a battery, would output the estimated energy contained within for a standard cell battery of 3.6 Volts. The constants needed for this estimation were taken from [7]. Finally a

script that ran the simulation for battery weights that ranged from .1 mg to 1 mg, 6 types of acids (Lead-acid, Alkaline long-life, Carbon-zinc, NiMH, NiCad, and Lithium-ion) as well as packet sizes up to 2^{10} was used to retrieve 660 simulation results.

B. Analysis

The primary focus of the simulation results had to do with the trade off between battery type, and the amount of time/packets sent required to complete deplete the initial energy source of the target Node. As we can see from the figures below, the results of running this simulation were not extremely surprising. This section will begin by listing the results for the Alkaline Long Life battery

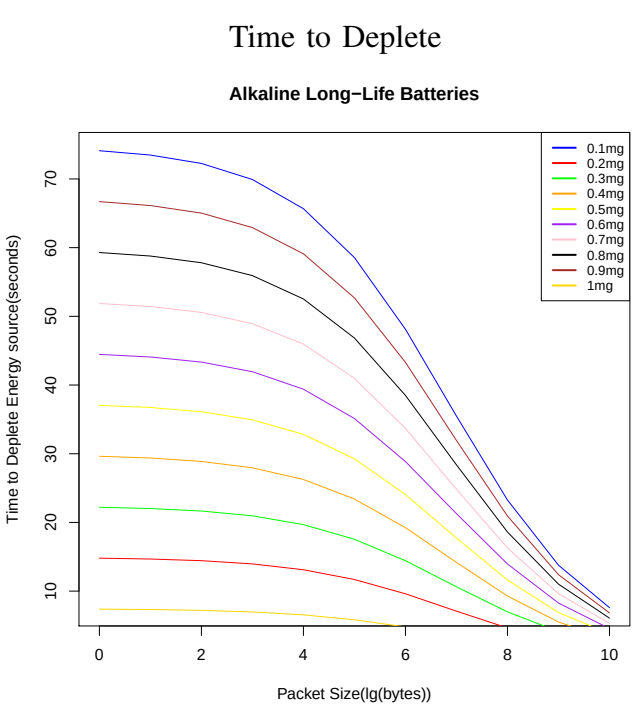


Fig. 3. The figure above represents a logarithmic regression of the number of bytes per packet sent on the x-axis, and the time required to completely deplete the initial energy of an Alkaline battery of various weights given an attacker who is transmitting to the receiving node once every ten milliseconds.

Because the simulations were run on packet sizes in powers of two, using a logarithmic regression on the x-axis allows us to more easily estimate the way the curves would look. Also, we realize that the data from the previous two graphs can be displayed on a single graph, but we ran out of time to display it this way. Below is the non regressed data for the same battery.

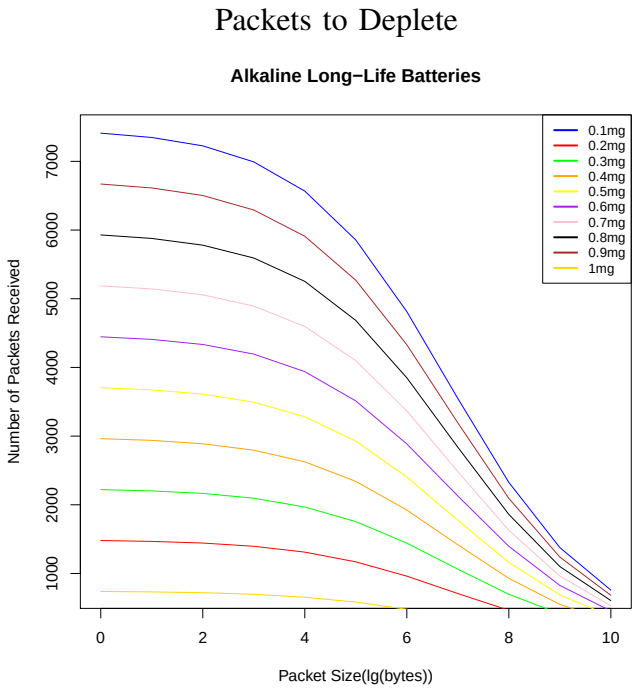


Fig. 4. This figure not surprisingly looks much like the previous figure, however, now we can see the number of packets sent on the y axis instead.

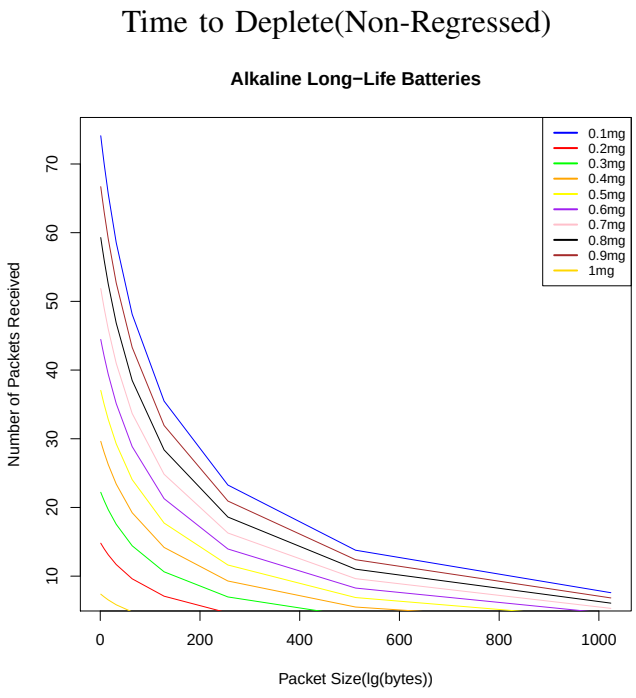
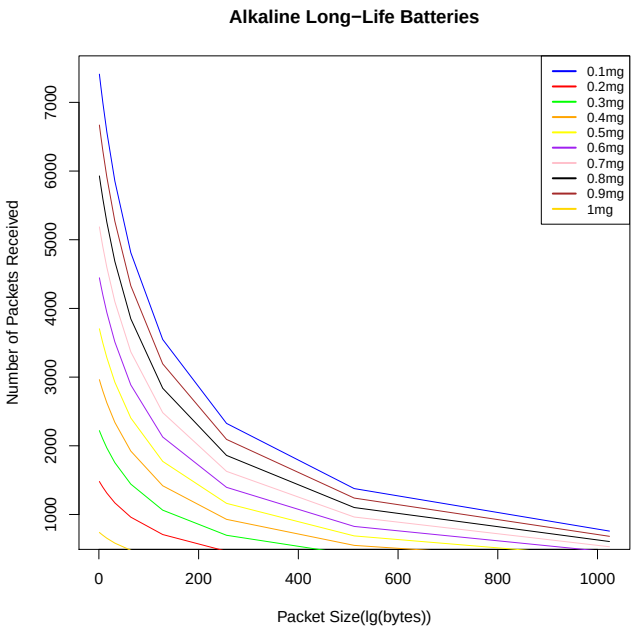


Fig. 5. It appears to be useful to look at the data in its non regressed from in some cases, as such the non regressed curves are displayed here for this particular battery.

The same results, and graphs were derived by using multiple different types of battery acid. One

Packets to Deplete(Non-Regressed)



thing that is clearly noticeable from the simulation results is that Packet Size has an interesting affect on the drain time for a battery. From the data we collected it appears that there is an inflection point on the graph around the point where x = 8.5. This is also the case for all of the battery types we simulated. We leave it to future work, to extend the packet size simulation out further, one reason we haven't investigated larger packet sizes is because after a packet size of 2048 bytes or greater, the target node would send an acknowledgment, and we only wanted power to be drained by the reception of packets, this limit can be raised to run future simulations under the same attack model for larger packet sizes.

IV. Conclusion

A. Future Work

After running these simulations there are a number of different ways we can go with our future work. One is to add more complexity to the simulation in order to gain deeper insight into how a wireless network of sensor nodes reacts to a power consumption attack. We could model the entire network of sensor nodes that the target node is connected to so that we can see how the whole network reacts to one of the nodes losing power. We can also implement and simulate different security protocols to see how they stand up to the attack. Since we already have the framework for this type of attack we can also research, model, and simulate additional attack methods.

We will also be doing a cost benefit analysis of the batteries for individual sensor nodes, that shows how likely a distributor is to use a larger battery with the hope of mitigating power consumption attacks on sensor nodes. We will also run similar simulations with different parameters varied, such as distance to transmit, and receive and more.

B. Remarks

In the current phase of our research, we have investigated the effects of variable battery types and weights on the time to consume all of a nodes energy. This is important for our future research, because it helps provide us with some introductory points. Meaning, we will be able to adapt what we have learned up to this point to continue our investigation, and run similar simulations under different assumptions. It also helped give us a starting point for the next consumption attack we will be modeling, as discussed in the methodology section.

C. Limitations

The most substantial limitations to this project were the amount of time we had to work, and the fact that there is a steep learning curve with NS3 simulator. Some future limitations we will most certainly be facing are: NS3 doesn't support the WLAN protocols we need to use, so we will have to approximate them in NS3 or use a different simulator. And again the time frame on this project is very limiting, it is my hope (at least), that this project can be carried to a certain point within the semester, and then to fruition in form of a publication beyond the end of the semester.

References

[1] S. Junnila, I. Defee, M. Zakrzewski, A.-M. Vainio, and J. Vanhala, "Uute home network for wireless health monitoring," in *Biocomputation, Bioinformatics, and Biomedical Technologies, 2008. BIOTECHNO '08. International Conference on*, June 2008, pp. 125–130.

[2] V. Manju, S. Senthil Lekha, and M. Sasi kumar, "Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks," in *Information Communication Technologies (ICT), 2013 IEEE Conference on*, April 2013, pp. 74–77.

[3] D. R. Raymond, R. Marchany, M. Brownfield, and S. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network mac protocols," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 1, pp. 367–380, Jan 2009.

[4] E. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless ad hoc sensor networks," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 2, pp. 318–332, Feb 2013.

[5] P. Barontib, P. Pillaia, V. W. C. Chooka, S. Chessab, A. Gottab, and Y. F. Hu, *Computer Communications*.

[6] "Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low rate wireless personal area networks (wpans)," *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pp. 1–320, Sept 2006.

[7] "All about batteries - energy," Mar. 2014. [Online]. Available: http://www.allaboutbatteries.com