Mitigating Power Consumption Attack Risk of Wireless Sensor Networks

Micah Thornton
mathornton@smu.edu

Ryan Sligh
rsligh@smu.edu

Bobby Santoski
rsantoski@smu.edu

ABSTRACT

The work presented in this paper examines two specific forms of power consumption attacks on Wireless Sensor Networks (WSNs). More specifically it attempts to discover possible risk mitigation strategies to use when faced with these types of attacks. The two forms of power consumption that are examined in this paper are the standard denial of sleep attack and a routing power draw attack. It was found that the routing power draw attack compromised sensor nodes much more quickly than did the standard denial of sleep attack. The various types of internal power sources that are used in sensor nodes were also examined. It was found that a Lithium-Ion battery was able to resist denial of sleep attacks for the longest amount of time. We conclude by suggesting that a wireless sensor network employer carefully consider the type of battery they use, as well as the need for routing in their network.

1. INTRODUCTION

1.1 Denial-of-Sleep Attacks

Firstly, it is important to note that the term "Denial-of-Sleep attack" refers to a general class of potential attacks. Second, this term is used to describe a sub-category of the Denial-of-service attack. A Denial-of-Sleep attack is defined as an attack that targets the energy supply of wireless nodes causing them to consume power rapidly. As Raymond, and Midkiff state in their paper, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", a denial of sleep attack specifically targets the primary power-draws in Wireless Sensor Networks[16]. In their paper: "Fighting Insomnia: a Secure Wake-up Scheme for Wireless Sensor Networks" R. Falk, and H. Hof Discuss the ways that this attack is orchestrated[4].

In a wireless sensor network the nodes generally have an "awake" state and a "sleep" state[4]. While The node is in the "awake" state it's wireless radio is turned on, and it is able to receive and send messages. Whereas a node that is asleep will only sense, and calculate. In the sleep state the receiver will not be active, and therefore the node's power draw is much smaller, because the power to calculate and sense is negligable compared to the power required to receive and send transmissions. The node is awakened in various ways depending on the design of the network, the network proposed by R. Falk et al. had a low power wake-up radio that caused nodes to switch to the "awake" state when they received a signal.

Denial-of Sleep attacks are effective against wireless sensor network nodes because they usually have smaller power supplies due to the need to be mass produced, and deployed in large numbers[18]. Wireless sensor nodes are generally designed simplistically for ease of use and set up, and as such are unable to make use of more sophistocated security mechanisms[13]. This entails the inability to fight certain forms of denial-of- sleep and denial-of-service attacks.

The perpetration of these attacks can take on many forms, several of which will be discussed in this paper. The first we will discuss is the most simplistic: an attacker targets one node by sending many packets and forcing the node to remain in the "awake" state, because it is continually receiving data. This attack was simulated with varrying packet sizes, and batteries to analyze the relationship, we will call it the "standard denial of sleep attack". A second attack that will be discussed is really a slight variation of the first, which takes into account the attackers knowledge of the protocols in use and by which an attacker may increase that knowledge[13]. A third attack uses an indirect approach to power consumption by sending a transmission from the attacker node, to an arbitrary network node, which gets routed by the targetted node, we refer to this attack as the "routing power draw attack". If the model were expanded to deal with many nodes on a network, the attacker might try to find the longest path in order to compromise the most nodes. Vasserman and Nicholas Hopper call this attack a stretch attack in their paper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks."[19]. The fourth form of denial of sleep attack that will be discussed is known as the "droplet" attack, which takes advantage of error checking on a noisy channel in wireless sensor networks[6]. The final form we will be discussing in this paper is the transmission of data from the attacker to a network of nodes which have a minimum bounded transmission power to help avoid a noisy channel.

1.2 Existing Mitigation Strategies

The most basic model that we discussed above describes a single attacker with unlimited power, and no knowledge of the security protocols used who is continuously sending transmissions to a wireless sensor node that has no lower noise bound, no random sleeping patterns, and is currently awake. This type of attack truly "Denies" the node the ability to sleep, as the node would sleep when it was no longer receiving transmissions. There are many mitigation strategies that would effectively reduce this risk including: a low power wake-up radio[4], a previously decided interval scheduling for transmissions and receptions among the nodes [13], and the method we will be testing is simply using a

larger battery.

The second attack discussed above has the same assumptions as the first, however the attacker knows either nothing or has limited information about the protocols used by the network. This attack was introduced in a paper by Raymond et al. where they discussed several mitigation strategies at length[13]. This can be mitigated by a jamming detection protocol that would catch authenticated messages, as they discuss.

The third attack by which the attacker targets a node that is used as a router can be mitigated by keeping track of the source of the traffic and forcing the node to go to sleep after so many messages are received from the same source consecutively within a certain short amount of time.

The fourth attack discussed is the "droplet" attack, which takes into account error checking in its effort to deplete the target nodes energy supply. He and Voigt discussed three specific mitigation strategies, among which were: allowing for handling of address in the hardware and dynamic channel switching to avoid an attacker on a single channel.

The fifth attack discuses a network which is in a noisy environment and has a minimum threshold for transmission power, which could be attacked by contributing a substantial amount to the noise level in the area, forcing the nodes to use more power when they transmit messages regularly. A potential mitigation strategy is to maximum noise level before all nodes halt awake state and go to sleep until a single node's low power receiver detects lower noise levels then it wakes up and wakes the entire network with transmissions. Using jamming protection protocols and interval scheduling as up above, also helps to mitigate this problem[13]

1.3 Other Relevant work

Because of their prevalence in solving many modern problems such as proximity monitoring, remote health monitoring[11], and surveillance WSN have accumulated a wide following in the research community. As they play a vital role their has also, unfortunately, been a lot of interest generated in the black hat community over compromising WSNs. A specific paper by Raymond et al. has bridged the gap between many different forms of WSNs and investigated the effects of specific attacks on the MAC sublayer[13]. Much energy efficient hardware has also been introduced to help mitigate these attacks[12]. Denial of sleep attacks also apply to the realm of any wireless ad hoc network, and there has been a large amount of work done in reference to mitigating attacks on these systems as well [19].

The purpose of denial of sleep attacks generally doesn't end after a single node is compromised, the effects of a single node failing due to running out of power have also been investigated.[1]. There have been some methods proposed that make use of a general recommendation discussed in this paper (including a renewable power generator I.e. a solar panel)[5].

As attacks on WSNs became more and more prevalent many publications outlining how these attacks are performed were written[2][16]. But the community also responded with many papers regarding defense mechanisms against specific attacks[15][3][14][7][8][17][10][9].

2. RESULTS AND ANALYSIS

2.1 Simulation Methodology

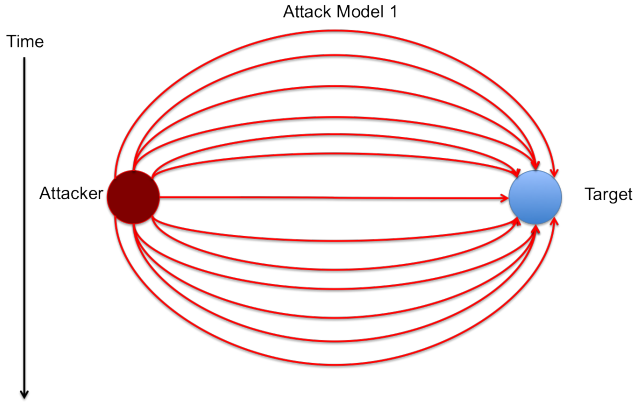
The key problem that we address is the mitigation of power consumption attacks on individual sensor nodes in wireless sensor networks. One central issue underlies the surface details of all wireless sensor nodes: a limited power supply. The nature of wireless sensor networks is such that it is likely optimal to draw power remotely, from a source such as a battery. The battery would also have to be quite small so it would not impede the actual duties of the node and take up space thereby rendering manufacture more costly and less effective.

We turned immediately to analyze the source from which the power was being drawn. Using a piece of software called NS3, we simulated the time required by the attacker to compromise a wireless radio by sending packets. The wireless radios were equipped with batteries that contained a certain internal acid. The acids tested are seen in the table in the next section. The weight of each battery was varied from 0.1 mg to 1 mg and 660 simulation results were collected.

Next, to gain a more thorough understanding of the implications of different kinds of power consumption attacks that are performed on WSNs we created a simulation environment in python, in which the user could define: the packet size (in bits), the initial energy in each node (in Joules), the power required to transmit packets (in Watts), the power required to receive packets (in watts), the speed of the transmission radios (in bits per second).

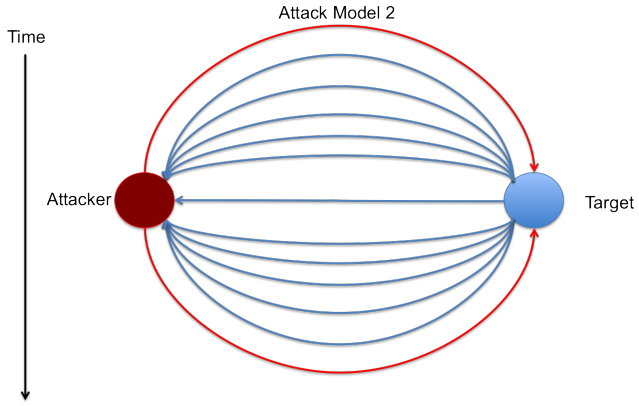
As stated in the introduction we specifically examined two attacks, the standard denial of sleep attack and the routing attack. Below are diagrams of what was simulated, and for the sake of completeness one attack that was not simulated.

Figure 1: Standard Denial-of-Sleep Attack



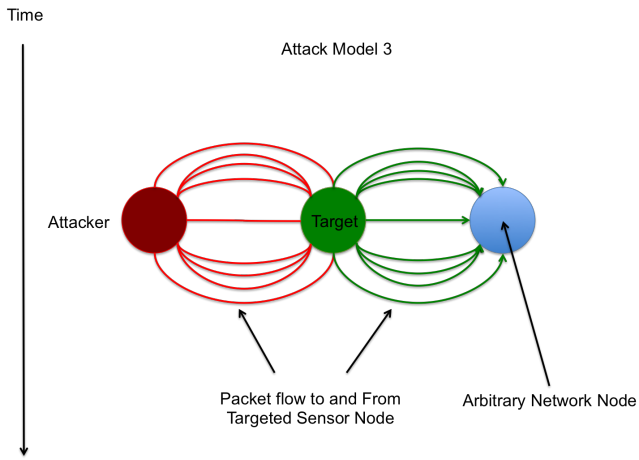
The image above depicts the "standard denial-of-sleep attack" the attacker continuously sends packets to the target to keep it in the "awake" mode so that power is drawn from the battery more quickly.

Figure 2: Inverse Denial-of-Sleep Attack



The image above depicts the "inverse denial-of-sleep attack" the attacker sends a request to the target to force it to transmit over and over again, this image represents a system where an acknowledgement is required after a transmission, but is never sent by the attacker we defer simulation of this form of attack to future work.

Figure 3: Routing Power Draw Attack



The image above depicts the "routing power draw attack" the attacker routes through the target node which causes the target to go through both transmitting and receiving procedures, it is a particularly vicious attack.

2.2 Simulation Results

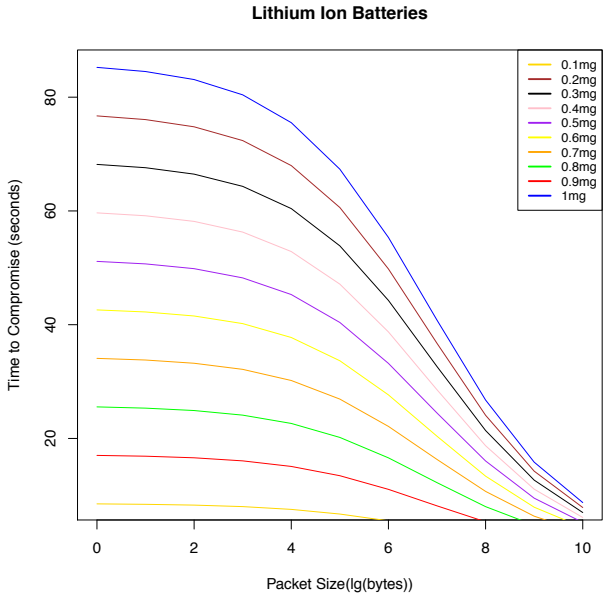
The first results came from running the standard denial of sleep attack on various different battery types, the size of transmitted packets varied in powers of two from the size of two bits to one kilo bit, and the packet transmission rate was constant at one packet every ten milliseconds.

Figure 4: Battery Compromise Table

B-Type	TTC(Min)	MTTC	TTC(Max)
Lead Acid	0.2789 s	9.8798 s	27.0307 s
Alkaline Long Life	0.7589 s	27.1017 s	74.1107 s
Carbon-Zinc	0.2489 s	8.7950 s	24.0700 s
NiMH	0.6489 s	23.0336 s	62.9907 s
Nickle-Cadmium	0.2689 s	9.4734 s	25.9207 s
Lithium-Ion	0.8689 s	31.1701 s	85.2400 s

In the table above "B-type" represents the type of acid that was tested, "TTC" represents the time to compromise (the time it takes to deplete all the energy from the sensor node), "MTTC" is the mean time to compromise. The batteries that are highlighted in blue showed a marginally better resistance to the standard denial-of-sleep attack, while those in red were compromised far too quickly to be implemented and deployed as effective defenses. As the table plainly shows the lithium-ion battery was the most resistant to the standard denial-of-sleep attack. Below we show how the change in packet size affected the time to compromise of the lithium-ion battery.

Figure 5: Time to Compromise for Battery Weights



Probably the biggest take away from this graph is the fact that all battery weights seem to converge in terms of time to compromise as the packet size being transmitted increases. From this graph we can tell that it would be more effective to use higher battery weights only when the packet sizes are kept relatively small. However, if the packet size is sufficiently large then it would be in the best interest of the distributor to choose a smaller weight.

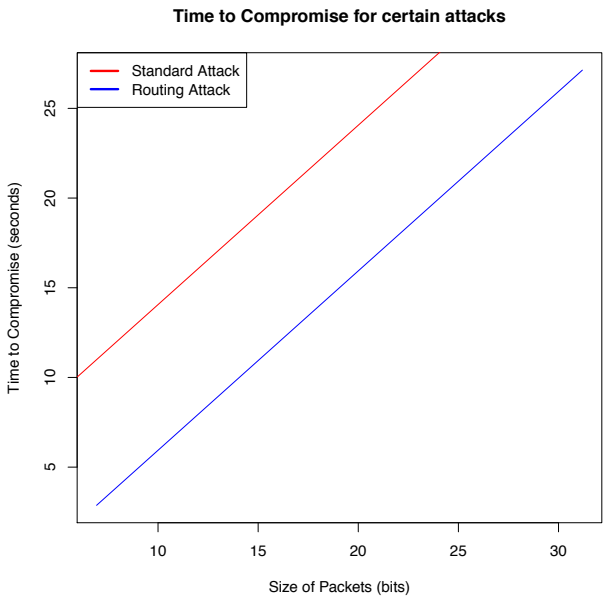
In our second simulation we tested the time to compromise a sensor node for two of the previously discussed attack, the standard denial-of-sleep attack and as well as the routing power draw attack. The table below shows some of the preliminary results from the second simulation.

Figure 6: Attack Comparison Table

A-Type	TTC(Min)	MTTC
Denial of Sleep	0.02558 s	14.49850 s
Routing Power Draw	0.02558 s	3.16868 s

From the table we noticed (not surprisingly) that the routing power draw attack compromised the sensor nodes much more quickly than the standard denial-of-sleep attack. We also plotted linear regressions of the time to compromise for each type of attack as the packet size increases. As we expected from the table the routing power consumption attacks is simply a linear transformation upwards of the standard denial of sleep attack, meaning that the derivatives of the two types of attacks are equivalent. That said, the rate of change with respect to packet size may be equivalent but the linear transformation upwards shows a strong indication that the routing power draw attack is more potent and worthy of consideration on the part of WSN employers.

Figure 7: Attack Comparison Chart



Because routing causes the target node to both transmit and receive simultaneously it is not surprising that routing can be a more effective power consumption attack. The simulation we used only examined a single target node. However, this attack could easily be easily extended using an algorithm that targets as many nodes as possible. It is important to note that the routing attack is entirely dependent on the individual protocols that WSN employers choose to implement.

3. CONCLUSION

3.1 Proposed Solutions

From our results we can draw two definite conclusions. As we have shown earlier there are numerous security protocols for wireless sensor nodes that aim to protect against specific types of power consumption attacks. These are effective for the attacks they are designed to defend against but provide little to no protection against other attacks. If one were to implement security protocols to defend against any attack that is known the cost of production for any one node quickly rises due to adding additional battery allocation and processing power for each defense. Furthermore this approach forces manufacturers to pick and choose which attacks they will be focusing on defending against, which can leave gaping security holes. Our first proposed strategy for mitigating power consumption attacks attempts to solve the problem at its most basic level, the power source. The idea of adding more power to sensor nodes is a simple yet effective mitigation strategy as it defends against all types of power consumption attacks. As shown in our tests, batteries such as the lithium ion can have dramatic effects in increasing the life span of a node when it is the target of a power consumption attack. Additionally, since adding more powerful batteries to every wireless sensor node is not always feasible, the idea of equipping a sensor node with a power regeneration device such as a solar panel or hydroelectric generator is an effective alternative. This has the same effect of adding additional battery with the benefit of having to be replaced much less. Depending on the circumstances of the implementation of any given wireless sensor network either of these methods of increasing battery life could benefit the network's security greatly.

Another conclusion that we can take away from our tests is that the routing power draw attack tested is much more potent than the standard denial of sleep attack tested. Therefore it is important to carefully consider routing procedures in a wireless sensor network. Routing in a wireless sensor network should not be a standard for all sensor networks as the inclusion of it forces a network to either take steps to implement additional security against the attack or open themselves up to a devastating attack possibility. Instead wireless sensor network deployers should examine whether or not routing is neccesary in their network at all. This especially applies to smaller networks that can get by without having to route packets. Though larger security conscious wireless sensor networks whose deployers are not able to implement defenses against a routing power draw attack would be better off reconfiguring their network to not have routing nodes.

3.2 Future Work

There are a number of different paths our research can take in the future. We can model and test additional attack types based on the simulations we have already created. These simulations have shown to give reliable results so it would be fairly easy to add new attack types. We can also do a cost benefit analysis of different types of batteries and alternative power sources for sensor nodes. For example we could compare the relative security benefit of a 1mg lithium ion battery with the security benefit of a small solar panel. From there we could find out which what is solution is most effective and the circumstances that can either add or detract from its effectiveness. Additionally we can compare the data we gather from the initial cost benefit anaylsis of the solutions to the cost benefit of previously introduced mitigation strategies. For instance we could see how the security benefit of a low power wake up radio, such as the one proposed in the paper "Fighting Insomnia: a Secure Wake-

up Scheme for Wireless Sensor Networks" by by R. Falk et al.[4] Lastly we can pursue additional research related to the neccesity of routing in wireless sensor networks and its alternatives.

4. REFERENCES

[1] Milan [Los Alamos National Laboratory] Bradonjic, Aric [Los Alamos National Laboratory] Hagberg, and Pan [Los Alamos National Laboratory] Feng. Performance of wireless sensor networks under random node failures. Jan 2011.

[2] M. Brownfield, Yatharth Gupta, and N. Davis. Wireless sensor network denial of sleep attack. In *Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC*, pages 356–364, June 2005.

[3] Chen Chen, Li Hui, Qingqi Pei, Lv Ning, and Peng Qingquan. An effective scheme for defending denial-of-sleep attack in wireless sensor networks. In *Information Assurance and Security, 2009. IAS '09. Fifth International Conference on*, volume 2, pages 446–449, Aug 2009.

[4] R. Falk and H. J Hof. Fighting insomnia: A secure wake-up scheme for wireless sensor networks. In *Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on*, pages 191–196, June 2009.

[5] Matthew R. Harvey and Ronald D. Kyker. *Development of a photovoltaic power supply for wireless sensor networks.* Jun 2005.

[6] Zhitao He and T. Voigt. Droplet: A new denial-of-service attack on low power wireless sensor networks. In *Mobile Ad-Hoc and Sensor Systems (MASS), 2013 IEEE 10th International Conference on*, pages 542–550, Oct 2013.

[7] Ching-Tsung Hsueh, Chih-Yu Wen, and Yen-Chieh Ouyang. A secure scheme for power exhausting attacks in wireless sensor networks. In *Ubiquitous and Future Networks (ICUFN), 2011 Third International Conference on*, pages 258–263, June 2011.

[8] Ching-Tsung Hsueh, Chih-Yu Wen, and Yen-Chieh Ouyang. Two-tier receiver-initiated secure scheme for hierarchical wireless sensor networks. In *ITS Telecommunications (ITST), 2012 12th International Conference on*, pages 254–258, Nov 2012.

[9] Xu Huang, M. Ahmed, and D. Sharma. A novel algorithm for protecting from internal attacks of wireless sensor networks. In *Embedded and Ubiquitous Computing (EUC), 2011 IFIP 9th International Conference on*, pages 344–349, Oct 2011.

[10] Xu Huang, M. Ahmed, and D. Sharma. Timing control for protecting from internal attacks in wireless sensor networks. In *Information Networking (ICOIN), 2012 International Conference on*, pages 7–12, Feb 2012.

[11] 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*, pages 125–130, June 2008.

[12] V.C. Manju, S.L. 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*, pages 74–77, April 2013.

[13] David R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff. Effects of denial-of-sleep attacks on wireless sensor network mac protocols. *Vehicular Technology, IEEE Transactions on*, 58(1):367–380, Jan 2009.

[14] David R. Raymond, R.C. Marchany, and S.F. Midkiff. Scalable, cluster-based anti-replay protection for wireless sensor networks. In *Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC*, pages 127–134, June 2007.

[15] David R. Raymond and S.F. Midkiff. Clustered adaptive rate limiting: Defeating denial-of-sleep attacks in wireless sensor networks. In *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1–7, Oct 2007.

[16] David R. Raymond and S.F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. *Pervasive Computing, IEEE*, 7(1):74–81, Jan 2008.

[17] R. Rughinis and L. Gheorghe. Storm control mechanism in wireless sensor networks. In *Roedunet International Conference (RoEduNet), 2010 9th*, pages 430–435, June 2010.

[18] Vladimir Shakhov and V. Popkov. Performance analysis of sleeping attacks in wireless sensor networks. In *Computational Technologies in Electrical and Electronics Engineering, 2008. SIBIRCON 2008. IEEE Region 8 International Conference on*, pages 418–420, July 2008.

[19] E.Y. Vasserman and N. Hopper. Vampire attacks: Draining life from wireless ad hoc sensor networks. *Mobile Computing, IEEE Transactions on*, 12(2):318–332, Feb 2013.