Denial of Service Attacks in Wireless Sensor Networks

Eric Bartocci & Justin Matthews

*Abstract*—Wireless Sensor Networks (WSNs) are on the rise. It is very likely that in the near future WSNs will be a part of daily use within some areas of industry. WSNs are limited when it comes to energy and communication, both having a very short range. The essence of attack-defend in WSNs security can be expressed by mutual strategies of interdependence while game theory can be used for the purpose of accounting for interactions among strategies of rational decision makers. With that said, security of WSNs is very intuitive. We will try to show just how challenging security is through game theory. This paper presents a survey of security approaches to the Denial of Service (DOS) attacks based on game theory in WSNs.

The main attack will focus on is Denial of Service (DoS) Attacks. Game theory can help researchers figure out the payoff of attackers in a network environment. There is a wide range of attacks that can be used on a WSN so fully securing a network is difficult. We will discuss how to prevent DoS attacks, Intrusion Detection Systems (IDS), fortifying security, and maintaining the network with defective nodes.

*Index Terms*—Wireless Sensor Networks; game theory; Wireless Sensor Networks security; intrusion detection; Denial of Services

# INTRODUCTION

Wireless sensory networks are a growing study in today’s world and can revolutionize warfare, homes, and electrical devices all together.   With everything becoming 'smart' and wireless, wireless sensory networks will be a very efficient way to charge devices and collect data efficiently. In today’s word everything is trying to become more mobile, while maintaining a wireless connection. Wireless sensory networks will help with the goal of staying connected. A WSN consists of several inexpensive, small nodes that make up a network topology. Since failure is inevitable in this network environment sensors must be deployed in large numbers. These nodes can collect data by using sensor technology to collect air pressure, weather, motion/movement, light, wind speed, noise, temperature, and location. These sensors can also recharge themselves by sending wireless electricity to help power nearby sensors. There are many factors to charging these sensors, perfect charging, and limited charging. With these new capabilities WSNs will become a fast growing network that will eventually become a part of everyday use.

Security with WSNs will become essential once this network topology is in use. In this paper we will focus on Denial of Service attacks on WSNs. DoS attacks could have a detrimental influence on a WSN. Intrusion detection is important. Along with intrusion detection we will talk about counter measures that can be taken to help once a DoS attack is recognized.

This paper will demonstrate this through a game theory approach. We will show how to strengthen a WSN with security. Our categories for this approach are: preventing DoS attacks, strengthening security, and coexisting with infected nodes. Each scenario will include just how easy it will be from an attackers stand point, and just how difficult it can be from a defender point of view. We will also discuss advantages and disadvantages from both sides.

DoS attacks are very harmful to Wireless Sensor Networks because of how versatile they can become. Implementation of a DoS attack can happen on the bottom 4 layers of the OSI reference model.

Figure 1 from reference [3]

“At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious

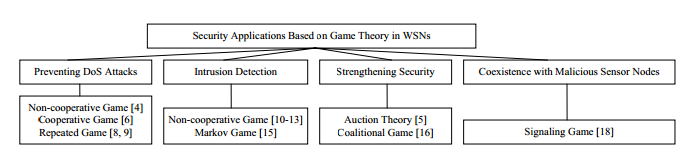
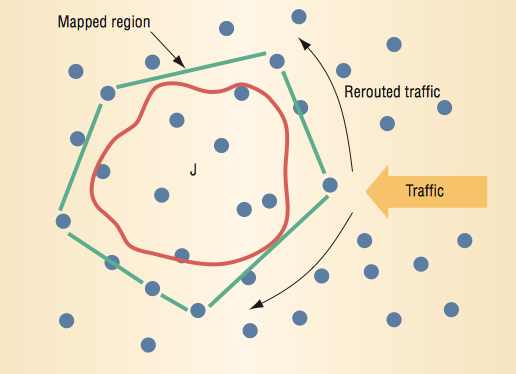


Figure 2 [2] Approaches based on Game Theory for WSN Security

flooding and de-synchronization”[1]. Since Wireless Sensor Networks most of the time are remote it is easy for nodes to be stolen or interfered with at any time. These attacks won’t be discussed because physical security is only held responsible by the initial setup. DoS attacks however, can be stopped by configuring the setup of the nodes.

# Denial of Service Strategies

A Denial of Service attack works by stopping any service by two or more devices. In Wireless Sensor networks these attacks can focus on stopping data communications as well as all power to the nodes. Since most sensor networks work by transferring energy to all the nodes from a base station attackers will focus on stealing or draining power to nodes.

That is one way out of many to attack these vulnerable nodes. Since the attack is so broad and there are many solutions. As many hardening techniques need to be implemented to achieve the highest payoff for our network. One of those techniques is a MAC admission control called rate limiting. “One solution makes the MAC admission control *rate limiting*, so that the network can ignore excessive requests without sending expensive radio trans- missions. This limit cannot drop below the expected maximum data rate the network supports, though. One design-time strategy for protection against battery-exhaustion attacks limits the extraneous responses the protocol requires. Designers usually code this capability into the system for general efficiency, but coding to handle possible attacks may require additional logic” [3]. Another very popular DOS attack is jamming of sensors.

Figure 3[3] Collaboration of Nodes.

In this Nash Equilibrium approach we seek to minimize the benefit of the attacker while maximizing the payoff for our nodes in the network. Nash Equilibrium is a solution that describes a steady state condition in the game. No player would want to change their strategy unless there is one that benefits the current player.

Let (S,F) be a game with n players

Si = strategy set for players I

S= S1 \* S2 \* . . . \* Sn Strategy profile

F = (F1(x) … Fn(x)) Is the payoff function

For x all inclusive S

The problem is fine tuning the results based on the game being played. By developing a matrix to represent Nash Equilibrium we can represent situations where the payoff is equal or a player is benefiting. There is an infinitely repeated game approach as well as a shorter and more harmul attack game. The infinite approach is what we will focus on because it is a more common game as to seek benefit for a long period of time, thus the attack receives information without being caught.

|  |  |  |
| --- | --- | --- |
|  | WSN Node Strategy A | WSN Node Strategy B |
| Attacker strategy A | 4/4 | 1/3 |
| Attacker  Stategy B | 3/1 | 2/2 |

Figure 4 Equilibrium Matrix

# Game Theory Approach

One method to solve the problem of Denial of Service attacks in by using Game Theory. Game Theory is a situation where there are two players that are working towards the same goal; however, sometimes they are working against each other. “A game generally consists of a set of players, a set of strategies for each player, and a set of corresponding utility functions. A strategy for a player is a complete plan of actions in all possible situations throughout the game. In any games, the players try to act selfishly to maximize their consequences according to their preferences” [2]. Game theory can be modeled after two players interacting and attempting to maximize their outcomes from one another.

For our Game Theory approach we will look at malicious sensor nodes refusing to forward incoming packets, a DoS attack. This approach came from our reference [2]. In [2] they look at WSNs as fully dynamic networks and all communication between clusters is through cluster heads. “An optimal payoff function that fulfills the objective for securing a sensor network based on cooperative game” [2]. Using figure 4 you can see the different payoffs of the attacker and actual sensor nodes. A very simple matrix but the Nash algorithm used with actual statistics can figure out a strategy profile for solving a DOS attack. Nash Equilibrium in figure 4's case is set on a coordination game where players base their strategy on the other player. The matrix is set up as the relative payoff for attacker / WSN Node with each combination. “To calculate the payoff between two sensor nodes, the authors consider a) sensor nodes’ distance, b) each sensor node’s transmitter signal strength, c) how many packets each sensor node receives and forwards at each time slot, and d) the trustworthiness of the traffic. The more the transmitter signal strength is, the more the sensor node cooperates with its neighbors. The cooperation between sensor nodes is defined as a function of the minimum signal strength for cooperation, and distance between the sensor nodes and the cost of packet forwarding” [3]. Security is measured by the percentage of exposed traffic if security is compromised, and cooperation is a big factor in passing information and power from sensors. The embedded operating systems like TinyOS, a WSN OS, is designed with real-time properties and uses event handlers and tasks to handle an event [4]. Stopping these few attacks knowing the other attackers move is essential to optimizing a Wireless Sensor Network. Knowing the other players move will help us transfer data and keep it out of their hands.

# Conclusion

Wireless sensor networks have many uses and will revolutionize the way that humans interact with each other, technology, and nature. Future research will help develop wireless Sensor Networks and make it Wireless sensor networks have many uses and will revolutionize the way that humans interact with each other, technology, and nature. With the variety of attacks on this topology, security is a very important aspect of deploying such a network domain. In this paper we have given approaches made by other researchers in solving jamming, infecting nodes, and others categorized as DoS attacks. Looking to the future we believe researchers will fully implement game theory into their solution methods to solve denial of service attacks on wireless sensor networks.

Acknowledgements

We would like to thank all of the researches from our sources for providing the research needed to complete this paper. With future study we believe that wireless sensor networks will become widely used across the globe.

References

[1]Al-Sakib K. P. , Hyung-Woo L. , Choong S. H., Security in Wireless Sensor Networks: Issues and Challenges, Feb 20, 2006.

[2 ]Shigen, S., Guangxue, Y., Qiying, C., & Fei, Y. (2011). A Survey of Game Theory in Wireless Sensor Networks Security. *Journal Of Networks*.

[3]Wood, A. D. and Stankovic, J. A., “Denial of Service in Sensor Networks”, Computer, Volume 35, Issue 10, Oct. 2002 pp. 54 - 62.

[4]Yenumula B R., Security Issues in Wireless Sensor Networks, 9-26-2011