Chapter 12
Applying Game Theory in Securing Wireless Sensor Networks by Minimizing Battery Usage

Mehran Asadi
The Lincoln University, USA

Afrand Agah
West Chester University of Pennsylvania, USA

Christopher Zimmerman
West Chester University of Pennsylvania, USA

ABSTRACT

In this chapter, the authors examine the impacts of applying game theory on the network throughput, network voltage loss, and accuracy of malicious node detection in wireless sensor networks. Nodes in a wireless sensor network use our proposed protocol when deciding whether or not to forward packets they receive from other sensors in order to conserve power. Wireless sensor network nodes achieve this by optimizing their decision-making based on a framework using game theory. Defining a suitable cost and profit for routing and forwarding incoming packets and keeping a history of past behaviors of non-cooperating nodes gradually forces malicious nodes out of the wireless sensor network.In this chapter, the authors examine the impacts of applying game theory on the network throughput, network voltage loss, and accuracy of malicious node detection in wireless sensor networks. Nodes in a wireless sensor network use our proposed protocol when deciding whether or not to forward packets they receive from other sensors in order to conserve power. Wireless sensor network nodes achieve this by optimizing their decision-making based on a framework using game theory. Defining a suitable cost and profit for routing and forwarding incoming packets and keeping a history of past behaviors of non-cooperating nodes gradually forces malicious nodes out of the wireless sensor network.

DOI: 10.4018/978-1-5225-2594-3.ch012

1. INTRODUCTION

A Wireless Sensor Network (WSN) consists of wireless sensors, small devices that collect data readings such as light or temperature from an environment. The sensors then send the data to a base station, a central location for data to congregate (Akyldiz, Sankarasubramaniam, Su, and Cayirci (2002)). Wireless sensor networks have potential to revolutionize the way in which the real world is monitored and controlled. Wireless Sensor networks impose a series of security challenges for network designers (Chong & Kumar, 2003). Among these security problems, Denial of Service (DoS) attacks, defined as any event that diminishes or eliminates a network's capacity to perform its expected function, degrade networks' intended services to its users. One simple form of a DoS attack is arbitrarily neglecting to forward some messages (Malekzadeh, Abdul Ghani, Subramaniam, and Desa (2011)).

A malicious node can drops messages on a random or arbitrary basis, but still participate in lower-level protocols, and may even acknowledge reception of data to the sender, Such a node is neglectful. The dynamic source routing protocol is susceptible to this attack (Eidenbenz, Kumar, and Zust (2006)). Because the network caches routes, communications from a region may all use the same route to a destination, and a malicious node can degrade or block traffic from a region to a base station (Karlof & Wagner, 2003).

Game theory has been used in various fields such as economics, politics and biology; it is a field of study that attempts to model decision-making (Osborne & Rubinstein, 1994). Game theory has previously been applied within the context of modeling multiple nodes in a wireless sensor network attempting to share a shared medium: their radio communication channels (Felegyhazi & Hubaux, 2007).

We incorporate game theory for the purpose of extending a sensor's battery life. This is accomplished by helping the sensors optimize their decision making process about whether or not to forward any data packets they may receive (Agah, Asadi, and Zimmerman 2011) and (Agah, Das, and Basu 2005). On one hand, if a node decides to never forward any packets, it conserves its available battery power, but no data flows through the network from that particular node. However, if a node forwards every packet that it receives, then node demonstrates its reliability and traffic flows through the network but the node will run out of battery power much faster than if the node were to not forward any of the incoming packets. By use of game theory, we attempt to extend a node's battery life while allowing it to forward an acceptable amount of packets through the network to have an optimum configuration (Asadi, Zimmerman, and Agah 2012).

We investigate how selfish behavior of individual players may affect the performance of the network as a whole. In a wireless sensor network, each node generates its own data and forwards incoming packets for others. Forwarding packets can consume a considerable amount of battery life. In this chapter we include the following features:

- **Game theory:** Game theory can provide insight into approaches for optimization. Often node decisions at a particular layer are made with the objective of optimizing performance at some other layer of the network. Game theory allows us to investigate the existence, uniqueness and convergence to a steady state point when network nodes perform independent adaptations. Using game theory helps us to design incentive schemes that lead to independent, self-interested participants towards outcomes that are desirable from a system-wide point of view (Machado & Tekinay, 2008).