A Game-theoretic Approach to Security and Power Conservation in Wireless Sensor Networks

Mehran Asadi[1], Christopher Zimmerman[2], and Afrand Agah[2]
(Corresponding author: Afrand Agah)
Center of Excellence in Business and Entrepreneurial Studies, Lincoln University[1]
Lincoln University, PA 19352
Department of Computer Science, West Chester University[2]
West Chester, PA 19383
(Email: aagah@wcupa.edu)

Abstract

In this paper, we investigate the impacts of applying game theory on the network throughput, network voltage loss and accuracy of malicious node detection to wireless sensor networks. We implement a protocol which the sensors use when deciding whether or not to forward packets they receive from other sensors in order to conserve power. Nodes in a wireless sensor network accomplish this by optimizing their decision making based on a framework using game theory. Defining a suitable cost and profit to routing and forwarding incoming packets and keeping a history of experiences with non-cooperating nodes drives malicious nodes out of the wireless sensor network.

Keywords: wireless sensors, game theory, security

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 the data to congregate [4]. Wireless sensor networks have potential to revolutionize the way in which the real world is monitored and controlled. Also, such networks impose a series of security challenges to network designers [11]. 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 vulnerability by arbitrarily neglecting to route some messages [25].

A subverted or malicious node can still participate in lower-level protocols, and may even acknowledge reception of data to the sender, as it drops messages on a random or arbitrary basis. Such a node is neglectful. The dynamic source routing protocol is susceptible to this attack [14]. 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 [21].

Game theory is a field of study that attempts to model decision making which has been used in various fields such as economics, politics and biology [31]. Game theory has previously been applied to wireless sensor networks, but within the context of modeling multiple nodes in the network attempting to share a shared medium: their radio communication channels [17].

We use game theory for the purpose of extending a sensor's battery life. We accomplish this by helping the sensors optimize their decision making process about whether or not to forward any data packets they may receive [1, 2, 3]. On one hand, if a node decides to never forward any packets, it conserves its battery power, but no data flows through the network. However, if a node forwards every packet that it receives, that 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 packets. By using game theory, we attempt to find an optimum configuration that will extend a node's battery life while still allowing the node to forward an acceptable amount of packets through the network [5].

It is our interest to investigate how selfish behavior by 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 traffic for others. Forwarding others traffic can consume a considerable amount of battery life. The contributions of this paper are therefore incorporating the following elements:

- **Game theory:** Often node decisions at a particular layer are made with the objective of optimizing performance at some other layer, therefore game theory can provide insight into approaches for optimization. It allows us to investigate the existence, uniqueness and convergence to a steady state point when

network nodes perform independent adaptations. It 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 [24].

- **Cooperation:** There is a trade-off between good cooperation and resource consumption; therefore nodes have to economize on their resources. At the same time, however, if they do not forward messages, others might not forward either, thereby denying service. Total non-cooperation with other nodes and only exploiting their readiness to cooperate is one of several boycotting behavior patterns. Therefore, there has to be an incentive for a node to forward messages that are not destined to itself [13, 14, 15, 22].

- **Reputation:** The performance of the network can reach an undesirable state due to the selfish behavior of individual wireless nodes. Therefore, incentives are proposed to steer nodes towards desirable operational equilibrium of the network behavior. We use a reputation system for incentivizing. Each node gains reputation by providing services (forwarding incoming packets) to others [26, 27]. Each node builds a positive reputation for itself by cooperating with others and is tagged as selfish or malicious otherwise. Reputation is maintained as a probabilistic distribution, enabling the node to have full freedom and not get constrained by some discrete levels of reputation as used in eBay, Yahoo auctions [35]. Note that reputation is not a physical quantity but it is a belief; it can only be used to statistically predict the future behavior of other nodes and cannot define deterministically the actual action performed by them [18].

- **Battery:** Recent technological advances within the field of wireless sensor networks have made it possible to support long-lasting operating lifetimes and large amounts of data transmission in wireless sensor networks. A major challenge is to maximize the lifetime of these battery powered sensors to support such transmissions. Battery powered sensors might waste a huge amount of energy if we do not carefully schedule and budget their discharging [10, 30].

This paper is organized as follows. Section II reports the related work. Section III formulates the game. Section IV evaluates the performance of the proposed protocol, and Section V concludes the paper.

2 Related Work

Numerous techniques have been proposed in recent years for estimating battery lifetime. In addition, a variety of strategies have been proposed to exploit battery characteristics for designing more battery friendly systems and communication protocols. Authors in [33] report on systematic experiments that conducted to quantify the impact of key wireless sensor network design and environmental parameters on battery performance.They evaluated the extent to which known electrochemical phenomena, such as rate-capacity characteristics, charge recovery and thermal effects, can play a role in governing the selection of key wireless sensor networks design parameters such as power levels and packet sizes. They have also analyzed the non-trivial implications of battery characteristics on wireless sensor networks power control strategies, and find that a battery-aware approach to power level selection leads to a 52% increase in battery efficiency.

The most work in this area relies on simulation of generic battery models.There are a number of approaches of energy management in sensor networks, including topology management and network layer optimization. Authors in [9] empirically examine the gain of battery runtime due to the battery recovery effect, and found this effect significant and dependent on duration. They also proposed a more energy-efficient duty cycling scheme that is aware of battery recovery effect, and analyzed its performance with respect to the latency of data delivery.

The benefit of behaving well is not obvious in the case of a delay between granting a favor and repayment, which is when nodes of a wireless sensor network forward packets for each other [7]. Defining a suitable cost and profit to routing and forwarding incoming packets and keeping a history of experiences with non-cooperating nodes drives malicious nodes out of the wireless sensor network. Reputation systems are being used in many systems to provide a means of obtaining a quality rating of participants of transactions by having all parties give each other feedback on how their activities were perceived and evaluated [28, 29]. In order to avoid centralized rating, local lists are maintained at each node and nodes can look up senders in their blacklist containing any node with a bad rating before forwarding anything to them [23].

Like in all shared-medium networks, medium access control (MAC) is an important technique that enables the successful operation of the network. To design a good MAC protocol for the wireless sensor networks, we have to consider energy efficiency since prolonging network lifetime for these nodes is a critical issue. Major sources of energy waste are collision, overhearing and idle listening [38]. Therefore periodic listening and sleep reduces energy consumption by avoiding idle listening.

3 Game Formulation

In this paper, we first aim to study the mathematical modeling of battery discharge behavior in a wireless sensor network. Each player tries to maximize its own benefit, which is the available battery of each individual node. However if a node forwards all incoming packets then over time the node would diminish its own energy reserves. Based on this, nodes have a tendency of not forwarding

packets and acting selfishly to conserve energy. Our goal [39, 40] in this paper is to give incentives to those nodes that participate in the network activities by forwarding incoming packets. Solving this problem means finding a Nash equilibrium [32] for the whole network, whereas each node is pre-programmed with a set of rules, maximizing the payoff for the entire network [12, 16].

We assume that each node has a discrete representation for its remaining energy, and the incentive for each node is to have a better reputation, where each node can be positively or negatively affected by its reputation. Over time, nodes with low reputation can be isolated and labeled as selfish/malicious nodes, and at each node, there is a trade-off between saving energy resources and maintaining their reputation.

A game is formulated as $G =< N, A, \{u_i\} >$where N is the set of players (decision makers), A_i is the action set of player i, $A = A_1 * A_2 * ... * A_n$ is the Cartesian product of the sets of actions available to each player, and $\{u_i\}$ is the set of utility functions that each player i wishes to maximize, where $u_i : A \rightarrow \Re$.

Our proposed framework enforces cooperation among nodes and provides punishment for non-cooperative behavior. We assume that the rational users optimize their profits over time. The key to solve this problem is when nodes of a network use resources, they have to contribute to the network life in order to be entitled to use resources in the future. The base station keeps track of the behavior of other nodes, and as they contribute to common network operation, their reputation increases. We are interested in solving a game by predicting the strategy of each player, considering the information that the game offers and assuming that the players are rational.

Authors in [36] has proposed a game theoretic framework for power control in wireless sensor networks, but their results only show the transmitting power versus the utility. Authors in [8] proposed an efficient power management in wireless sensor networks but they have only presented the average coverage. In this paper we demonstrate the actual voltage loss of the network in the presence of malicious nodes as well as utility and the accuracy of malicious node detection.

3.1 Equilibrium

We formulate a model that captures a situation in which two bargainers have the opportunity to reach agreement on an outcome in some set X and perceive that if they fail to do so then the outcome will be some fixed event D. Here the set X is the set of feasible divisions of positive reputation and D may be the event in which neither party receives any positive reputation. The set of Nash equilibria of a bargaining game of alternating offers is very large. One such equilibrium is that in which both players always proposes x^* and always accept a proposal x if and only if $x = x^*$. For any agreement x and period t, there is a Nash equilibrium for which the outcome is the acceptance of x in period t. One such equilibrium is that in which through period $t-1$, each player demands the maximum reputation and rejects all proposals, and from period t on proposes x and accepts only x [31]. The procedure we study is one in which the players alternate offers in periods of the game, each period t represents one round of bargaining. The first move of the game occurs in period 0, when player 1 makes a proposal (forward my incoming packet), which player 2 then either accepts or rejects. Consider the Nash equilibrium in which both players always propose x^* and player i accepts a proposal x in period t if and only if $(x, t) >_i (x^*, t)$. In the equilibrium player 2's strategy dictates that in any period he rejects such a proposal x, this threat induces player 1 to propose x^*. Players 2's threat is incredible, given player 1's strategy: the best outcome that can occur if player 2 carries out his threat to reject x is that there is agreement on x^* in the next period, an outcome that player 2 likes less than agreement on x in period 0, which he can achieve by accepting x. The base station increments the reputation of nodes at periodic intervals. If a node rejects a proposal (forwarding a packet) neither party receives a positive reputation from the base station.

Acceptance ends the game, while rejection leads to period 1, in which player 2 makes a proposal (increase my reputation), which player 1 has to accept or reject. Again, acceptance ends the game; rejection leads to period 2, in which it is once again player 1's turn to make a proposal. There is no limit on the number of rounds of negotiations [31]. The fact that some offer is rejected places no restrictions on the offers that may subsequently be made. In particular, a player who rejects a proposal x may subsequently make a proposal that is worse for him than x. If no offer is ever accepted then the outcome is the disagreement event.

We assume each player cares only about whether an agreement is reached and the time and content of the agreement, not about the path of proposals that preceded the agreement. We will define a bargaining game between nodes of wireless sensor network, and by finding the solution; we mathematically guarantee the best strategy for forwarding incoming packets, while keeping a good reputation and saving battery life of each node.

Maximizing cooperation between nodes and minimizing battery usage at each node are the two main goals that we investigate in the above game theoretic framework. Any breach of cooperation results in packets being dropped; therefore, partial cooperative strategy never leads to an equilibrium point. Meanwhile boundary conditions can be set to achieve cooperation in a network of selfish nodes. Our goal is to propose a strategy that is more adaptive to full cooperation after a nodes misbehavior. It is important to realize that even malicious attacks are carried out by an attacker after seeking the cooperation (unknowingly) of other non-malicious nodes in the network.

We stimulate nodes to contribute to the network operations in order to be able to use network services, therefore nodes receive incentives for cooperation. We also

seek to minimize battery usage; the decrease in available battery level must discourage nodes from overloading the network but not to the limit that they do not cooperate with the rest of the network for their selfish act of energy utilization. Therefore we need to design a cooperative security mechanism that enforces cooperation and shows that when no countermeasures are taken against misbehaving nodes, network operation can be heavily jeopardized. Also we capture and describe battery usage behavior at each node, and based on this battery model we present a battery-aware strategy for each node to avoid energy loss but gain better reputation over the course of the game.

3.2 Payoff and Reputation

Each node i has a von Neumann-Morgenstern utility function defined over the outcomes of the stage game G, as $u_i : A \rightarrow \Re$, where A is the space of action profiles [32]. A's action profile space is listed as:

$$A = \begin{cases} Forward\ packets & A_1 \\ Do\ not\ forward\ packets & A_2 \end{cases}$$

Let G be played several times and let us award each node a payoff which is the sum of the payoffs it received in each period from playing G. Here,

$$u_i^t = \alpha r_i^t - \beta c_i^t$$

where r_i^t is the gain of node i's reputation, c_i^t is the cost of sending or forwarding a packet for the node as energy loss, and α and β are weight parameters. We assume that measurement data can be included in a single message that we call a packet. Packets all have the same size. The transmission cost for a single packet is a function of the transmission distance [34].

At time t, each node calculates the utility to be gained for each of the two actions available. For forwarding a packet, the utility is calculated as:

$$u_{A_1}^t = T * r_i^{t+1} - B * (c_s + c_r)$$

where r_i^{t+1} is the predicted gain of node i's reputation.

For sending a packet, c_i^t is broken down into two constant values: c_s and c_r. c_s is the voltage cost to send a packet and c_r is the voltage cost to receive a packet. B is the weight parameter for cost, and represents the importance of being conservative about sending packets when a node has a low battery leave. At a node's highest battery level, B will be 1. As the node's battery level crosses designated thresholds by decreasing, B will increase.

T is the weight parameter for the gain component of the equation and represents the number of units of time since node i has last forwarded a packet. T starts at 1 for each node i and increments every time any node i decides to not forward a packet. When a node sends a packet, T is reset back to 1. If a node has recently sent a packet, it may not be important to send another packet right away, which is why T starts at a low value. But as time passes without forwarding any packets, it is important that a node sends data through the network, which leads T to increase.

Table 1: Parameters and Notations

Cost of forwarding packet at node i	c_i
History at node i	h_i
Rating of node i	ρ_i
Reputation at node i	r_i
Utility at node i	u_i
Voltage cost of sending	c_s
Voltage cost of receiving	c_r
Weight Parameters	α_i, β_i, B, T

The utility for not forwarding a packet is calculated as:

$$u_{A_2}^t = T * 0 - B * c_s$$

Since there is no gain in reputation when not sending a packet, the gain is 0. However, receiving a packet from another node still costs energy.

After calculating the utility for each of these actions, the node will perform the action that yields the greater utility.

The strategy for each node i at time t is:

$$s_i(h^t) = \begin{cases} Forward & \text{if } u_{A_1}^{t+1} > u_{A_2}^{t+1} \\ Do\ not\ forward & \text{otherwise} \end{cases}$$

In order to compute the values of a node's gain, we turn our attention to the work proposed in [26]. In this work the authors proposed the concept of subjective reputation, which reflects the reputation calculated directly from the subject's observation. In order to compute each node's reputation at time t, we use the following formula:

$$r_i^t = \sum_{k=1}^{t-1} \rho_i(k)$$

where $\rho_i(k)$ represents the ratings that the base station has given to node i, and $\rho_i \in [-1, 1]$. If the number of observations collected since time t is not sufficient, the final value of the subjective reputation takes the value 0. The base station increments the ratings of nodes on all actively used paths at periodic intervals. An actively used path is one on which the node has sent a packet within the previous rate increment interval. Recall that reputation is the perception that a person has of another's intentions. When facing uncertainty, individuals tend to trust those who have a reputation for being trustworthy. Since reputation is not a physical quantity and only a belief, it can be used to statistically predict the future behavior of other nodes and can not define deterministically the actual action performed by them.

Table 1 depicts the notations that were used throughout this paper.

3.3 Configurations

We use three major network configurations. The first configuration, named case1, consists of a network of wireless sensors which broadcast packets to any nodes within range. Since the nodes in our experiment are located within a small distance of each other, all nodes in the network are capable of broadcasting directly to every other node in the network. Whenever a node receives a packet from another node and forwards the packet, that packet is re-broadcast to every node within range. For networks of a large size, this generates a large amount of traffic. In an attempt to remedy this, another network configuration was developed [20].

Case2 utilizes a neighbor system. Each node has a neighbor table that holds the IDs of several neighbors, which are determined by a handshaking process that occurs after the nodes boot up and send an initial voltage reading to the base station. The neighbor relationship is bi-directional. Whenever a node receives a packet, it checks the data. This gives the ID number of the node that just sent the packet. If the ID found in path of the packet is not found in the neighbor table of the receiving node, the node ignores the packet and no further action is taken. However, if the ID of the node that just forwarded the packet matches an ID in the neighbor table, then the node's number of packets received is incremented and the node will take the appropriate action with the packet. Since we did not have access to a large testing area where we could spread the nodes out further, this is an attempt to emulate a less dense, less traffic-heavy network than what is found in case1.

The third network configuration utilizes cluster networking. The network consists of groups of sensors called clusters, where the sensors in a cluster report to a sensor in the network that is designated as the cluster-head of the network. All non cluster-heads within a cluster, known as members of a cluster, only communicate directly with their respective cluster-heads. Cluster-heads transfer data to the base station where the data is to be collected and stored [6]. In our simulations, the process of determining which cluster-head a sensor reports to is based on the sensor's battery level. If a member receives a packet broadcast by a cluster-head within range, the member will forward that packet directly to its cluster-head.

For each configuration, simulations are run both with and without implementing game theory. By doing so, we can compare average network throughput, as well as voltage loss, and see under which scenario using one would be favorable over the other. The sensor programs for the game theory and non game theory configurations are identical except that the game theory program implements the strategy of whether or not to forward a packet that it receives. For the first two configurations, the networks are either entirely comprised of nodes that implement game theory or entirely of nodes that do not implement game theory. When we implement game theory in the cluster networking configuration, only the cluster-heads implement game theory.

For each game theory and non game theory configuration, simulations of networks consisting of entirely normal nodes were run, as well as simulations of networks containing varying percentages of malicious nodes. A node that acts maliciously is one that randomly drops packets in order to conserve its energy. For malicious non game theory nodes, before forwarding a packet the node randomly decides whether or not it wants to not forward the packet. For malicious game theory nodes, the node randomly decides whether or not it wants to not forward the packet before the strategy is applied.

For the first two network configurations, the sizes of the test networks start at 5 nodes, then increase by 5 up to 30 nodes. This allows us to observe what trends occur in reputation, voltage loss, and utility as the size of the network increases considerably. For the cluster networking configuration, all tests are run with a network size of 30 nodes.

3.4 Malicious Node Detection

In our simulations, we introduce malicious nodes into the network to see how they affect the network and if there is a way to detect and neutralize such nodes. Malicious nodes randomly drop packets, reducing the throughput of the network. Malicious nodes also consume additional power when randomly deciding whether or not to drop packets.

The base station keeps track of the reputation of each node in the network. Periodically, the base station will decide whether or not a node is acting malicious based on its throughput. The base station takes the current reputation of each node in the network and calculates the average, as well as the standard deviation. If a node's reputation is lower than the average minus the standard deviation, that node is deemed malicious. The base station sends a packet to that node ordering the node to turn its radio off and shut down.

4 Performance Evaluation

In the case1 scenarios, the simulation starts with an initial voltage reading from each sensor. In this work we have used MICAZ sensors [19], which run on TinyOs [37]. Next, a packet is broadcast once every 200 milliseconds for 300 seconds. Then a final voltage reading is sent to the base station. In the case2 scenarios, after the initial voltage reading, the neighbor handshaking phase takes place. After the neighbor handshaking process, each node broadcasts data once every 200 milliseconds for 300 seconds. Lastly, a final voltage reading is sent to the base station. In the cluster networking scenarios, an initial voltage reading is sent from each sensor. Next, cluster membership is established for each non clusterhead node in the network. After that, a packet is broadcast once

every 200 milliseconds for 300 seconds. Afterward, a final voltage reading is sent to the base station.

During the simulation, if a node receives a packet it will forward it or apply the game theory strategy, depending on the scenario. After sending the packets, each node turns its radio off for 10 seconds to get rid of the traffic in the network. Then, every node turns their radio on and sends one final voltage packet to the base station. This gave us a clear start and end voltage for calculating voltage loss. For malicious node detection, the base station checks to see if any nodes are malicious after 60 seconds into the simulation, and then once every 30 seconds after that. Any nodes that are deemed as malicious are turned off via radio.

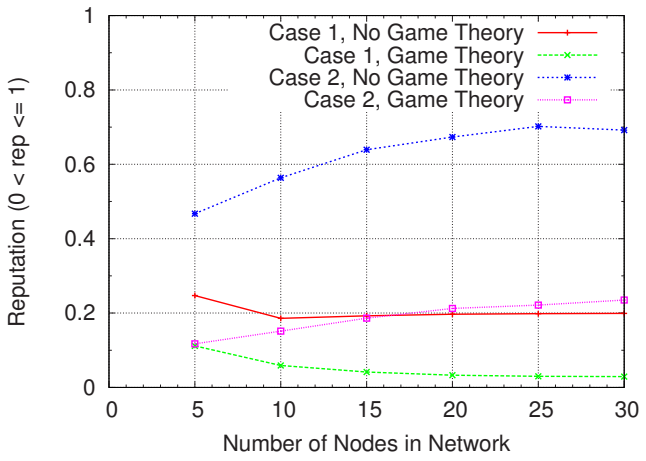

Figure 1: Average network throughput for normal nodes.

As shown in Figure 1, reputations for simulations using game theory have a lower reputation, than simulations not using game theory, regardless of network size. By implementing game theory, the average throughput of the network drops, but this is to be expected since the sensors are dropping packets based on a set of rules in order to save power.

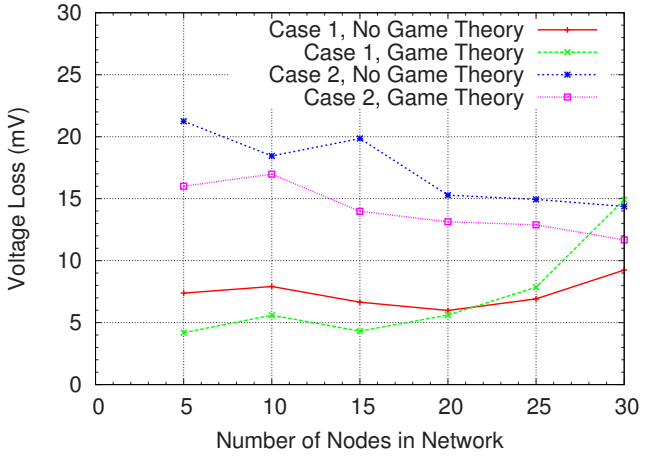

Figure 2: Average network voltage loss for normal nodes.

Figure 2 shows that for case1, implementing game theory results in a lower voltage loss for smaller networks, but results in a greater voltage loss for larger networks. As the size of a network increases, so does the traffic. Since deciding whether or not to forward a packet by using a strategy also consumes power, there is a point where the frequency of deciding whether or not to forward an incoming packet is so high that the energy used for implementing the strategy is greater than the amount of energy the node tries to save by not forwarding packets. For case2, implementing game theory consistently results in a lower network voltage loss. The neighbor system helps reduce the amount of traffic in the network, which prevents the voltage loss that happens with larger networks in case1.

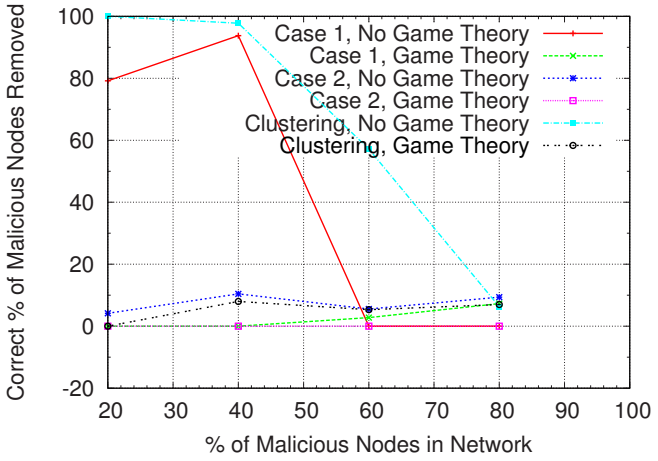

Figure 3: Average percentage of malicious nodes correctly removed from network.

As indicated by Figure 3, our procedure for detecting malicious nodes works best for networks containing small amounts of malicious nodes. Since malicious nodes usually have a lower reputation, if there is a small number of them present in the network, it is easier to detect them. However, if normal nodes in a network typically have low reputations, or if many nodes in the network have lowered reputations, it is difficult to detect malicious nodes because they don't stand out.

Figure 4 shows that our procedure for detecting malicious nodes raises a low percentage of false positives. For the most part, a small amount of false positives are raised, aside from case1 game theory scenarios. Since the nodes in the case1 game theory scenarios typically have a low reputation and there are less normal nodes in the network as the number of malicious nodes increases, the percentage of false positives detected increases.

As seen in Figure 5, average reputations for game theory cases are lower than non-game theory cases, except for the clustering scenarios, where reputation is higher by using game theory in networks with a larger percentage of malicious nodes.

As seen in Figure 6, in most cases, voltage loss is lower with game theory implemented than if not, even with the presence of malicious nodes.

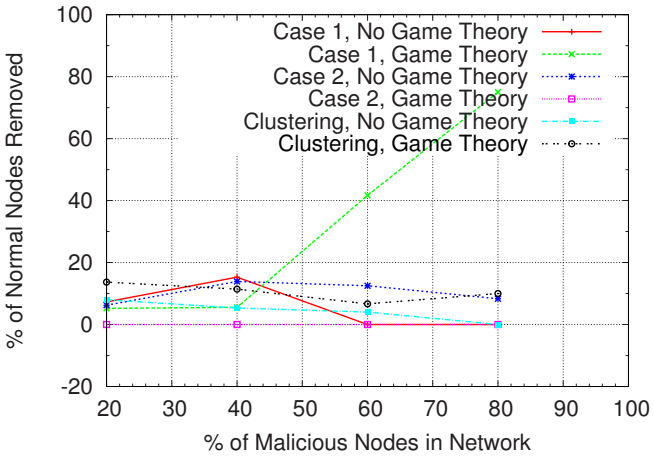

Figure 4: Average percentage of normal nodes incorrectly removed from network.

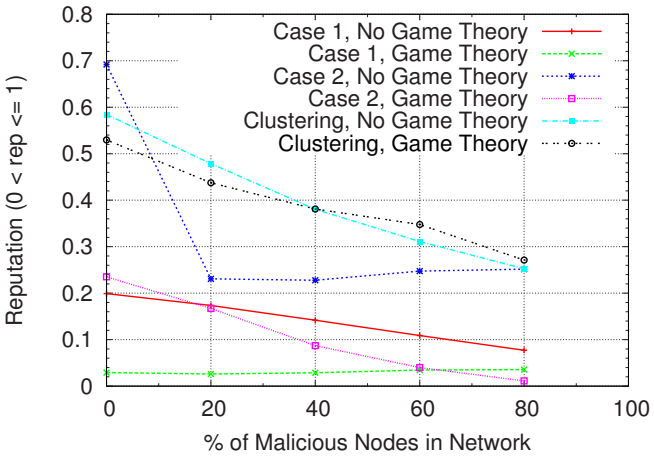

Figure 5: Average network throughput for malicious nodes.

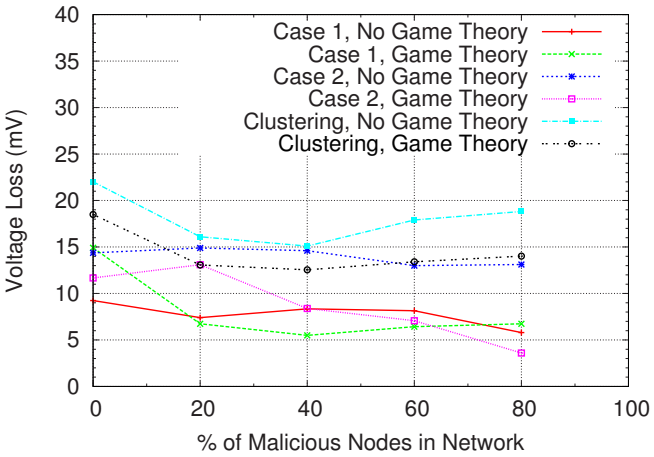

Figure 6: Average network voltage loss for malicious nodes. Broadcast(case 1), hop-by-hop(case 2).

Due to how we model utility in our project, utility is bound to decrease. Therefore, a better utility is not defined by how quickly it can rise, but rather how slowly it can decrease. As seen in Figure 7, for our case1 scenarios, utility for networks implementing game theory have a lower utility than those which do not implement game theory. However, this is caused by the high amount of traffic in a larger network.

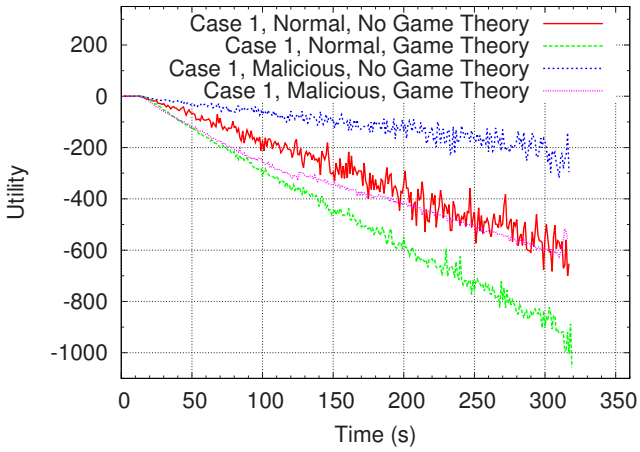

Figure 7: Average network utility for Broadcast (case 1) scenario (Network size - 30 nodes).

As seen in Figure 8, for our case2 scenarios, utility for networks implementing game theory have a higher utility than those which do not implement game theory. Despite the large network size, the neighbor system reduces the amount of traffic that flows through the network.

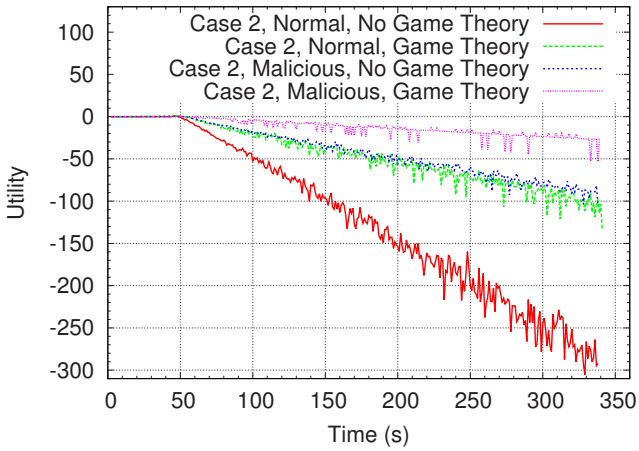

Figure 8: Average network utility for hop-by-hop (case 2) scenario (Network size - 30 nodes).

Figure 9 shows that, by implementing game theory, the average utility is higher than when game theory is not implemented in cluster networks.

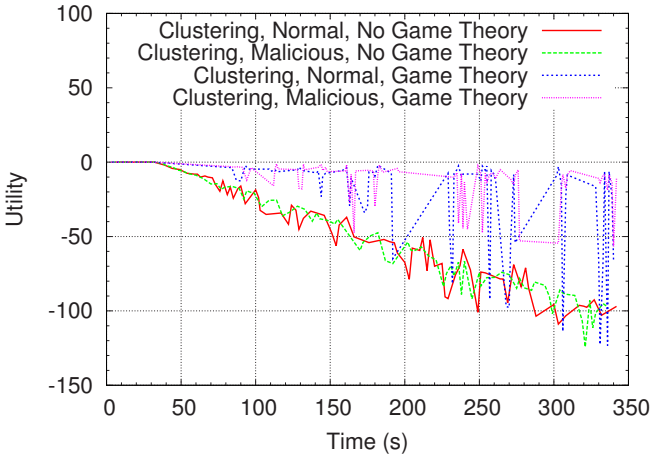

Figure 9: Average network utility for clustering scenarios (Network size - 30 nodes).

5 Conclusion and Future Work

Our results indicate that, under most cases, implementing game theory in a WSN is beneficial by helping reduce the amount of voltage consumption throughout the network. By adding a decision making process of when to send and not to send packets, the sensors conserve energy while maintaining the throughput.

Further work includes experimenting with different strategies in order to save power, as well as improving the accuracy of our malicious node detection procedure. Other possible extensions of this project would be to experiment with packets of different priorities and implement coalitions of nodes, also implementing different mechanisms for selection of cluster heads.

Acknowledgements

This work is supported by the National Science Foundation under grant number 1054492.

References

[1] A. Agah, M. Asadi, and C. Zimmerman, "Maximizing battery life: Applying game theory to wireless sensor networks," *The WCU Research Consortium*, 2011.

[2] A. Agah, S. K. Das, and K. Basu, "Enforcing security for prevention of dos attack in wireless sensor networks using economical modeling," *Proceedings of the 2nd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS)*, 2005.

[3] A. Agah, S. K. Das, and K. Basu, "Preventing dos attack in sensor and actor networks: A game theoretic approach," *IEEE International Conference on Communications (ICC)*, 2005.

[4] I. F. Akyldiz, Y. Sankarasubramaniam W. Su, and E. Cayirci, "Wireless sensor networks: A survey," *Journal of Computer Networks*, vol. 38, 2002.

[5] M. Asadi, C. Zimmerman, and A. Agah, "A quest for security in wireless sensor networks: A game theoretic model," *The International Conference on Wireless Networks (ICWN)*, 2012.

[6] S. Bandyopadhyay and E. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," *INFOCOM*, 2003.

[7] S. Buchegger and J. L. Boudec, "Nodes bearing grudges: toward routing security fairness and robustness in mobile ad hoc networks," *Proceedings of the 10th Euronicro Workshop on parallel, Distributed and Network-based Processing*, 2002.

[8] E. Campos-Nanez, A. Garcia, and C. Li, "A game-theoretic approach to efficient power management in sensor networks," *Operations Research*, vol. 56, no. 3, pp. 552–561, 2008.

[9] C. Chau, M. H. Wahab, F. Qin, Y. Wang, and Y. Tang, "Battery recovery aware sensor networks," *the 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, 2009.

[10] M. Chi and Y. Yang, "Battery-aware routing for streaming data transmissions in wireless sensor networks," *Springer Science and Business Media, LLC*, 2006.

[11] C. Chong and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenge," *Proceedings of the IEEE, Special Issue on Sensor Networks and Application*, vol. 91, no. 8, 2003.

[12] G. V. Crosby, L. Hester, and N. Pissinou, "Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks," *International Journal of Network Security*, vol. 12, no. 2, pp. 107–117, 2011.

[13] S. Eidenbenz, L. Anderegg, and R. Wattenhofer, "Incentive-compatible, energy-optimal, and efficient ad hoc networking in a selfish milieu," *Proceedings of the 40th Hawaii International conference on system Sciences (HICSS)*, 2007.

[14] S. Eidenbenz, V. S. Kumar, and S. Zust, "Topology control games for ad hoc networks," *ACM Mobile Networks and Application*, vol. 11, no. 2, 2006.

[15] S. Eidenbenz, G. Resta, and P. Santi, "The commit protocol for truthful and cost-efficient routing in ad hoc networks with selfish nodes," *IEEE transactions on mobile computing*, vol. 7, no. 1, 2008.

[16] M. Felegyhazi, L. Buttyan, and J. P. Hubaux, "Equilibrium analysis of packet forwarding strategies in wireless ad hoc networks: the static case," *Proceedings of Personal Wireless Communications*, 2003.

[17] M. Felegyhazi and J. P. Hubaux, "Game theory in wireless networks: A tutorial," *EPFL - Switzerland, LCA-REPORT*, 2007.

[18] S. Ganeriwl and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks,"

ACM workshop on Security of Ad Hoc and Sensor Networks, 2004.

[19] MEMSIC Inc., "Micaz wireless measurement system," *http://www.memsic.com*.

[20] L. Chang J. Zhan and S. Matwin, "Privacy preserving k-nearest neighbor classification," *International Journal of Network Security*, vol. 1, no. 1, pp. 46–51, 2005.

[21] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *First IEEE International Workshop on Sensor Network Protocols and Applications (SPNA)*, 2003.

[22] D. Levin, "Punishment in selfish wireless networks: A game theoretic analysis," *Workshop on the Economics of Networked Systems*, 2006.

[23] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks," *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, 2003.

[24] R. Machado and S. Tekinay, "A survey of game-theoretic approaches in wireless sensor networks," *Elsevier Computer Networks Journal*, vol. 52, 2008.

[25] M. Malekzadeh, A. A. Abdul Ghani, S. Subramaniam, and J. Desa, "Validating reliability of omnet++ in wireless networks dos attacks: Simulation vs. testbed," *International Journal of Network Security*, vol. 123, no. 1, pp. 13–21, 2011.

[26] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," *Communications and Multimedia Security Conference*, 2002.

[27] P. Michiardi and R. Molva, "Game theoretic analysis of security in mobile ad hoc networks," *Research Report, Institute Eurecom*, 2002.

[28] P. Michiardi and R. Molva, "Prevention of denial of service attack and selfishness in mobile ad hoc networks," *Research Report RR-02-063, (Institute Eurecom)*, 2002.

[29] P. Michiardi and R. Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks," *European Wireless 2002: Next Generation Wireless Networks: Technologies, Protocols, Services and Applications*, 2002.

[30] P. Nurmi, "Modeling energy constrained routing in selfish ad hoc networks," *International conference on Game Theory for networks(GameNets)*, 2006.

[31] M. Osborne and A. Rubinstein, *A Course In Game Theory*. The MIT Press, 1994.

[32] G. Owen, *Game Theory*. NY: Academic Press, 2001.

[33] C. Park, K. Lahiri, and A. Raghunathan, "Battery discharge characteristics of wireless sensor nodes: An experimental analysis," *IEEE SECON*, 2005.

[34] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall, 2002.

[35] P. Resnick, K. Kuwabarra, R. Zeckauser, and E. Friedman, "Reputation systems: Facilitating trust in e-commerce systems," *Communications of the ACM*, vol. 43, no. 12, 2000.

[36] S. Sengupta, M. Chatterjee, and K. Kwiat, "A game theoretic framework for power control in wireless sensor networks," *IEEE Transactions on COmputers*, vol. 59, no. 2, 2010.

[37] TinyOS, "Tinyos documenatation," *http://docs.tinyos.net*.

[38] J. Heidemann W. Ye and D. Estrin, "An energy efficient mac protocol for wireless sensor networks," *IEEE INFOCOM*, 2002.

[39] C. Zimmerman, A. Agah, and M. Asadi, "Applying economical modeling to wireless sensor networks for maximizing the battery life," *The 26th Pennsylvania Computer and Information Science Educators (PACISE) Conference*, 2011.

[40] C. Zimmerman, A. Agah, and M. Asadi, "Incorporating economical modeling to extend battery life in wireless sensor networks," *Graduate Research and Creative Projects Symposium*, 2011.

Mehran Asadi obtained his Ph.D. degree in Computer Science from the University of Texas at Arlington. Dr. Asadi's scholarly interests include Economical Modeling of Security Protocols, Security in mobile ad-hoc networks, Machine Learning and in particular hierarchical reinforcement learning. Dr. Asadi has presented his research at several national and international conferences. He was also PI for a grant from Hewlett Packard and Co-PI for a grant from National Science Foundation. He has been reviewer for the journal of information science and in addition, he has contributed as a reviewer for handbook of computer networks by John Wiley and sons.

Christopher Zimmerman received his master degree in Computer Science from West Chester University of Pennsylvania.

Afrand Agah obtained her Ph.D. degree in Computer Science from the University Texas at Arlington. She is executive board member for Pennsylvania Association Computer and Information Science educators. In addition to her work on security in wireless sensor networks, Dr. Agahs scholarly interests include security and trust in pervasive computing and security in mobile ad-hoc networks. Dr. Agah has contributed as a committee member for various national and international conferences such as IEEE International workshop on wireless and sensor networks security; the International conference on wireless networks; IEEE communications society conference on sensor and ad-hoc communications and Networks; the IEEE wireless communications and networking conference; the Asian International mobile computing conference; and the IEEE International conference on high performance computing. She also served as a reviewer for a number of journals such as the journal of mobile communication, computation and information; the International journal of network security. In past she has also contributed as a reviewer for handbook of information security, and the Internet Encyclopedia, by John Wiley and sons.