

Uniform Sensing Protocol for Autonomous Rechargeable Sensor Networks

Volodymyr Pryyma, Ladislau Bölöni, and Damla Turgut
School of Electrical Engineering and Computer Science
University of Central Florida
Orlando, FL 32816-2362
{vpryyma, lboloni, turgut}@eecs.ucf.edu

ABSTRACT

Autonomous rechargeable sensor networks are becoming a feasible solution to many real world applications. In this paper, we propose a Uniform Sensing Protocol for autonomous rechargeable sensor networks. Our protocol aims to provide uniformly distributed sensing throughout the entire life-time of the network, thus increasing the overall network reliability. It considers the amount of available energy in the environment as well as the probability of encountering a specific number of threats. Using these parameters, each node estimates its own active period, such that uniform sensing is established. We compare the performance of our protocol with static and dynamic active time slot approaches. The simulation results show that the Uniform Sensing Protocol generates fewer failures and has a significantly longer mean time to failure than the other two schemes.

Categories and Subject Descriptors

C.2.2 [Computer-Communication Networks]: Network Protocols—*applications, protocol verification*

General Terms

Algorithms, Performance, Reliability

Keywords

Autonomous sensor networks, rechargeable sensors, uniform sensing

1. INTRODUCTION

Recent advances in the field of wireless sensor networks (WSNs) have made these types of networks popular solutions to many real-world applications. Some approaches require that a WSN be self-sufficient, meaning that it must operate successfully without any human intervention beyond initial deployment of the sensor nodes. The reasons behind

this may include various hazards to human life as well as difficulties gaining physical access to individual sensors. Additionally, some WSN applications require the network to be operational for indefinite periods of time, making efficient power management a priority. Thus, the problem is twofold: 1) a WSN requires a way to organize and schedule the sensor nodes in an autonomous manner, and 2) a WSN requires an efficient, rechargeable energy system in order to sustain its operations indefinitely.

An autonomous network structure, specifically designed for WSNs, was proposed by Olariu et al. [12]. This work focuses on developing an architecture that allows a WSN to operate unattended. All the data collected by the sensors is processed locally in the network, as opposed to being forwarded to a remote site. This autonomous structure allows the WSN to report any interesting behavior, or observation, to the client in a timely manner.

In order to prolong the lifetime of any WSN, rechargeable sensors can be used. There exists a variety of technologies for harvesting energy from the environment. Srivastava et al. [8], Paradiso and Starner [15], and Raghunathan and Chou [16] discuss a number of energy scavenging techniques. However, using any of the rechargeable methods does not automatically guarantee perpetual sensor operation because the rate of energy consumption is usually greater than the recharging rate. Thus, the sensors will run out of energy at some point in time, unless a careful energy management system is employed.

In this paper, we present a rechargeable implementation of the autonomous network architecture introduced by Olariu et al. In addition, we propose a Uniform Sensing Protocol for sensor nodes with energy scavenging capabilities. The focus of our protocol is on providing reliable sensor scheduling, such that the network experiences uniformly distributed coverage regardless of the current energy state. We implement the autonomous network structure using YAES simulator and compare the performance of our protocol with two other rechargeable schemes, one where the active time slot of sensor nodes is constant, and another where the active time slot is dynamically adjusted.

The rest of this paper is organized as follows. We begin by summarizing previous work on various rechargeable schemes and autonomous network structures. In Section 3, we present our uniform sensing protocol. Section 4 discusses the results of our simulation study. Finally, we conclude in Section 5.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

MSWiM'08, October 27–31, 2008, Vancouver, BC, Canada.
Copyright 2008 ACM 978-1-60558-235-1/08/10 ...\$5.00.

2. RELATED WORK

The idea of rechargeable sensors has been around for some time. Paradiso and Starner [15] discuss several energy scavenging technologies for mobile and wireless electronics. A number of power management issues for energy harvesting embedded systems are addressed by Raghunathan and Chou [16] and Srivastava et al. [8]. Jiang et al. [4] describe the hardware aspects of establishing perpetual environmentally powered sensor networks. However, to the best of our knowledge, implementing rechargeable nodes with an autonomous network structure has not been attempted before.

The AutoNomous networked sEnsoR system (ANSWER) by Olariu et al. [12] presents a conceptual foundation of how such an autonomous network functions. It is assumed that the micro-sensor nodes in this architecture possess certain capabilities, including a pseudo-random number generator, initial set of seeds for the number generator, a set of tuples, a perfect hash function, and initially synchronized clock. ANSWER uses a unique clustering system to organize the micro-sensors. The clustering approach uses wedges and coronas to create a coordinate system and partition the area around each Aggregation and Forwarding Node (AFN) into a number of clusters. Olariu et al. [13, 14] present the details of how such coordinate system is established and how clusterheads are elected. Furthermore, Wadaa et al. [17] show that once a coordinate system is established, it is possible to train the sensor network in order to minimize the cost of routing and data fusion. We implement the ANSWER architecture with rechargeable nodes and our uniform sensing protocol using YAES simulator [1].

Byers and Nasser [2] propose a utility-based decision-making process to maximize the lifespan, and in turn average utility, of a sensor network. This decision-making process enables the sensor nodes to change their roles over time and to dynamically adjust the routing paths in order to efficiently load balance the energy consumption in the network. In contrast, the sensor nodes in our protocol autonomously manage their energy budget to provide uniformly distributed sensing.

Kar et al. [9] introduce a dynamic node activation scheme, which is specifically designed for networks with rechargeable sensors. At any given time, each rechargeable sensor node is in one of the following states: active (normal operation), passive (battery recharging), or ready (waiting for job assignment). The authors show that their dynamic activation scheme is distributed, requiring only local state information, and performs very close to the global optimum. Our protocol employs a similar activation system, however more emphasis is applied on providing a reliable network coverage.

An adaptive duty cycling algorithm, introduced by Hsu et al. [3], allows rechargeable nodes to autonomously adjust their duty cycle based on energy availability in the environment. Performance tasking as well as several power management systems for rechargeable sensors are presented by Kansal et al. [5, 6, 7]. Our protocol adjusts the active time slot of each sensor based on available energy as well. However, once the length of the active period is established, it does not change, so that uniform sensing is maintained.

Zhu and Ni [19] propose a probabilistic wakeup protocol for wireless sensor networks. The central idea behind this protocol is to reduce the duty cycle of individual sensors, while exploiting the dense deployment of sensor networks. A distinct characteristic of this protocol is the fact that the

system ensures that the delay of detecting any event occurring in the network area is statistically bounded. Our protocol relies on the probability of an individual sensor node to encounter a number of threats. We employ Gaussian distribution to generate these probabilities.

A scheduling algorithm that relies on the battery capacity of the sensors is presented by Moser et al. [10]. A dynamic reconfiguration scheme for rechargeable sensor networks is proposed by Nahapetian et al. [11]. Our approach uses similar concepts to manage the energy budget of each sensor.

Zafar and Corkill [18] propose a two-phase scheme for estimating a solar harvesting model in situated agents. In the pre-deployment phase, the agents learn as much as possible about their environment patterns. This reduces the amount of learning each agent has to perform during actual deployment. Thus, once in the deployment phase, the agents simply complete their harvesting model. Our protocol, on the other hand, establishes the harvesting model entirely after deployment.

3. PROPOSED PROTOCOL

3.1 Problem definition

A rechargeable sensor network system has the same goal as a battery-based system when it comes to power management. In both cases, the network tries to manage power consumption as efficiently as possible in order to prolong the overall life-time of the network. However, while a battery-based system has to minimize the energy consumption of individual nodes, a rechargeable system usually strives to achieve operation under *energy equilibrium*, where the energy consumed does not exceed the energy harvested from the environment. Once the equilibrium point is reached, the sensor network can operate for indefinite period of time, restricted only by the hardware limitations.

Let $E_a(t)$ represent the available, or stored, energy of a single sensor node at time t , $E_c(t)$ represent the consumed energy, $E_h(t)$ represent the harvested energy, and $E_{leak}(t)$ represent the constant energy leak. Then, the *energy equilibrium* condition can be modeled as

$$E_a(t) - \int_0^T [E_c(t) - E_h(t)] dt - \int_0^T E_{leak} dt \geq 0 \quad (1)$$

where $T \in [0, \infty)$. Once this condition is satisfied across all sensor nodes, the network will be able to operate indefinitely without any interruptions resulting from sensors running out of energy.

In this paper, we present a protocol that takes full advantage of the rechargeable capabilities of the sensor nodes in order to provide uniformly distributed sensing across the entire network. Our approach is based on the individual sensor's ability to compute and manage its energy budget. Each sensor takes into consideration the amount of available energy as well as the probability that the sensor will encounter a certain number of threats.

3.2 Energy availability assumptions

Before going into details of our protocol, we describe the assumptions we make regarding the energy availability in the environment. The most efficient way to harvest energy from the environment is through converting solar energy into stored electrical energy [8, 15]. Thus, we assume that the

sensor nodes are equipped with special hardware for collecting solar energy. Furthermore, we assume that more energy is available for harvesting during the day than during the night period. We denote $r_{day}(t)$ as the recharging rate for the day period and $r_{night}(t)$ as the recharging rate for the night period. Thus, the following inequality always holds true

$$r_{day}(t) > r_{night}(t) \quad (2)$$

This assumption is representative of the real world environment. Solar energy is much more scarce at night time. As a result, the night period offers much less energy for scavenging by the rechargeable sensor nodes.

Additionally, we assume that $r_{day}(t)$ and $r_{night}(t)$ are not constant and tend to change during their respective time periods. As an example, consider a situation where clouds move in to cover a portion of the sensor network. Such cloud cover during day time will most likely decrease the recharging rate of sensor nodes. These changes in energy availability may have a lasting effect on the overall system performance depending on their duration. Our protocol takes into account these changes in available energy and adjusts the energy budget of individual sensors accordingly.

3.3 Autonomous network organization

In order to establish an autonomous network structure with our protocol, we implemented the ANSWER architecture proposed by Olariu et al. [12]. ANSWER consists of a large collection of sensor nodes, whose primary actions include continuous environment monitoring. In addition to performing various sensing operations, the sensors also have low power data processing and short range wireless communication capabilities. Since the sensor nodes are harvesting solar energy from the environment, they are able to maintain connectivity and functionality of the network for indefinite periods of time.

In addition to sensor nodes, ANSWER uses other, more powerful, nodes to efficiently organize the network. These nodes are referred to as Aggregation and Forwarding Nodes, or simply AFNs. The AFNs are either stationary, or mobile nodes that organize the sensors in their vicinity. Each AFN acts as a training agent and sets up a dynamic coordinate system centered around itself. AFNs have special equipment for long range communications and are responsible for processing the information received from the sensor nodes. We assume that the AFNs also have an infinite supply of energy.

ANSWER employs a unique coordinate system that allows for dynamic network reconfiguration and provides a simple and low-cost clustering scheme for organizing the sensor nodes. The dynamic coordinate system divides the surrounding area into *coronas* and *wedges*. Coronas are concentric circles of increasing radii that are centered at the AFN. The radius of each corona is determined by differential transmission power. All coronas have the same width, which is set to be slightly less than the transmission range of the sensor nodes. Wedges are equiangular dividers that originate at the AFN and extend to its full transmission range. The wedges are obtained using directional transmission. This coordinate system is dynamic in nature because it can be easily re-established in order to accommodate changes in network topology.

The ANSWER architecture provides the means for activating select subsets of sensor nodes at any given time, so that energy is conserved by the sensors that do not neces-

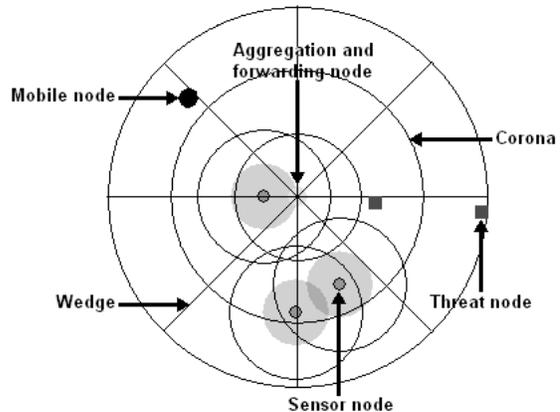


Figure 1: Screen shot of ANSWER implementation in YAES.

sarily have to be involved in the current sensing process. To accomplish this, the individual sensor nodes are activated based on a coloring scheme. Using the signal strength readings obtained during the establishment of the network, each node is assigned a specific color. The result is that the corona segments are further subdivided into a number of color sets. The color sets are numbered in the same order in each corona. Thus, the entire network is partitioned into a set of color graphs, such that all the sensors in any one graph are represented as vertices with the same color, and any two vertices within the transmission range of each other are connected by an edge.

Once the network is established, a trusted mobile node can move around in the network while communicating with the AFNs. The mobile node has specific goals, such as safely getting from one point in the network to another. Thus, the mobile node periodically communicates with the AFNs to check for possible threats that may interfere with its progress. In our case, a threat is considered to be an enemy vehicle capable of destroying the mobile node. The AFNs, in turn, perform task scheduling for the sensors under their control. If a threat is detected by a sensor, the threat's approximate position is first reported to an appropriate AFN, and then relayed to the mobile node. Based on the information reported by the AFNs, the mobile node can adjust its path in order to avoid all the threats. A screen shot of ANSWER implementation using YAES simulator is shown in Figure 1. More details on the ANSWER architecture and its functionality can be found in [12, 13, 14, 17].

3.4 Static active time slot approach

We consider three rechargeable schemes for a network under ANSWER's organization in order to prolong network life-time indefinitely. First, let us examine a very basic approach of dealing with rechargeable nodes.

While active, all rechargeable devices undergo energy consumption at some rate, $d(t)$. At the same time, rechargeable devices also experience some rate of energy gain, $r(t)$, provided that there is some amount of energy in the environment available for scavenging. Due to high energy consumption tasks such as transmission and data processing, and due to the low efficiency of harvesting energy from the

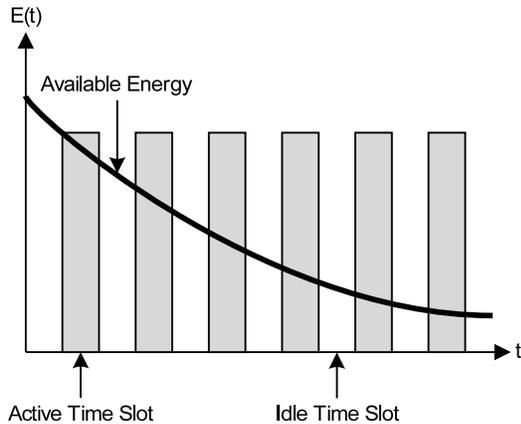


Figure 2: Static active time slot sensor activation.

environment, devices such as rechargeable sensors will always experience $d(t) > r(t)$. As a result, a rechargeable sensor node will most likely run out of energy at some point in time and will have to remain inactive until its battery is recharged to a certain level.

In order to prevent individual nodes from completely running out of energy, the amount of time during which the nodes are active has to be carefully managed, such that the nodes are allowed to stay idle for certain amounts of time and hopefully achieve operation under *energy equilibrium*. If we designate the maximum length of a time slot during which a sensor is allowed to stay active as T_{active} , then one obvious solution is to limit T_{active} to some constant value. This way, a sensor node will undergo periodic shifts from the active state to the idle state and vice-versa.

Ideally, a sensor in the idle state would be able to recover all of the consumed energy from the previous active state. However, this is rarely the case in real world applications due to reasons presented above. Additionally, deciding on appropriate length of T_{active} is a challenging task. Choosing a large value for T_{active} will likely cause sensors to deplete their energy supply very quickly, while choosing small T_{active} may leave the sensors in the idle state for too long, thus missing a number of important events. This is clearly shown in Figure 2, where the vertical bars represent the active state of the sensor nodes.

One major drawback of this protocol is the lack of adaptability. Since the available energy in the environment is likely to vary with time, the constant active time slot protocol will degrade as the available energy in the environment diminishes.

3.5 Dynamic active time slot approach

In order to compensate for the shortcomings of the static active time slot approach, we can dynamically adjust the length of the active period. In order to do so, each sensor node is required to calculate the length of its own active time slot based on several inputs. These input parameters consist of the length of the previous active time slot, the amount of currently stored energy in a node, the probability of encountering a threat, and the number of one-hop neighbors. The equation for calculating the length of the next active time

slot is as follows

$$T_{active}^{new} = T_{active}^{old} \frac{r^{new}(t)}{r^{old}(t) + r^{new}(t)} + \frac{E(t)}{\alpha \cdot d(t)} + C_{th} + C_n \quad (3)$$

The recharging rates $r^{new}(t)$ and $r^{old}(t)$ change with time to reflect the change in available energy for harvesting in the environment. $E(t)$ is the amount of stored energy a sensor node has at time t . $d(t)$ is a rate at which the nodes consume energy. α is a modification parameter that depends on the amount of stored energy in a sensor. Basically, α is a positive integer multiplier if the stored energy in a node is above fifty percent of total capacity, and a negative integer multiplier otherwise. C_{th} is a modifier that depends on the probability of encountering a threat. This modifier increases gradually each time a threat is detected and decreases every predefined time interval during which no threats were observed. Finally, C_n is a modifier that depends on the number of one-hop neighbors a node has. The value of C_n increases with increasing number of neighbors.

Based on the above equation, it is clear that the length of the active time slot will decrease when the node has little stored energy, and increase when the node has a lot of stored energy. The modifiers C_{th} and C_n further impact the length of the active time slot so that the active period is increased if the probability of encountering a threat is high, and decreased if there are many other sensor nodes nearby.

In contrast to static active period approach, the nodes with dynamic active time slot protocol do not consume all of their energy. Instead, the nodes reach a saturation region where they consume about the same amount of energy that they are able to harvest from the environment. The drawback to this approach is that there exist gaps in the network which an intruder might exploit. For example, during the day time most sensors will have a large active period due to abundance of solar energy in the environment. However, once night comes, the sensors will reduce their time spent in the active state in order to bring down their energy consumption. Thus, intruders will have a major advantage when they attempt to sneak into the network area during night time. Figure 3 clearly demonstrates this fact.

3.6 Uniform sensing protocol

Both the static and dynamic active time slot protocols focus on minimizing energy consumption by individual nodes. In contrast, we propose a protocol in which the sensor nodes use up most of their energy reserves in order to achieve uniform sensing throughout the entire network. Our protocol takes into consideration the amount of available energy in the environment and the probability that a node will encounter a certain number of threats. Based on these parameters, each sensor calculates its own energy budget and chooses T_{active} such that most of the energy is consumed in a single day and night cycle, which we designate as T_{cycle} .

In Uniform Sensing Protocol, the sensor nodes first calculate their energy budget at the beginning of each day and night cycle. Once this is accomplished, the length of the active time slot is estimated as

$$T_{active} = \frac{E(t)}{k(d(t) - 2r(t))} \quad (4)$$

where $E(t)$ represents the amount of currently stored en-

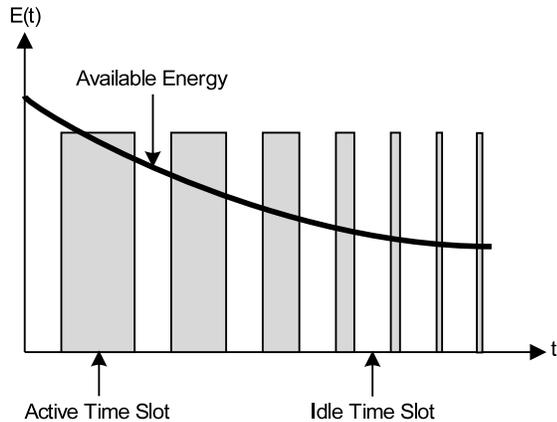


Figure 3: Dynamic active time slot sensor activation.

ergy in a sensor node, and $d(t)$ and $r(t)$ are the rates of energy consumption and gain respectively. The coefficient 2, in front of the recharging rate, corresponds to the fact that a node is gaining energy during both active and idle states. The parameter k represents the number of active and idle slots experienced by a sensor in a single day and night cycle. The number of active slots in a single cycle increases with increasing value of k . However, the length of a single active slot decreases with increasing k .

The parameter k has to be chosen a-priori and has to satisfy the following condition

$$kT_{active} \leq T_{cycle} \quad (5)$$

The value of k also depends on the probability that a sensor node will encounter a certain number of threats. If a sensor has high probability of encountering only a few threats, then the value of k can be reduced such that active periods are longer but less frequent. On the other hand, if a sensor node has high probability of encountering many threats, then the value of k can be increased in order to have more active time slots.

The Uniform Sensing Protocol uses a Gaussian distribution function to generate the probabilities of encountering threats. Since Gaussian distribution is not bounded, we estimate these probabilities to simplify our simulations. We employ a normal distribution function with four standard deviations, which includes 99.997% of all possibilities as shown in Figure 4. Using this method, the probabilities are generated based on the threat encounters from the previous cycles.

Once the sensor nodes calculate their respective probabilities of encountering threats, as well as their energy budget, they compute corresponding T_{active} and begin sensing. If a sensor does not encounter any threats, then its T_{active} will remain unchanged throughout the entire day and night cycle. At the onset of a new cycle, each node will recompute its threat probability and energy budget, as well as set a new value for T_{active} .

However, once a sensor encounters a threat, it will extend the length of T_{active} for as long as it can sense that a threat is present. Once a threat moves out of the sensing range, the sensor node will recompute its energy budget, based on the

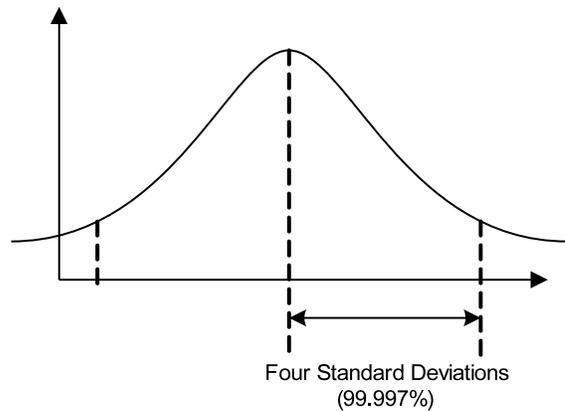


Figure 4: Estimate of Gaussian distribution.

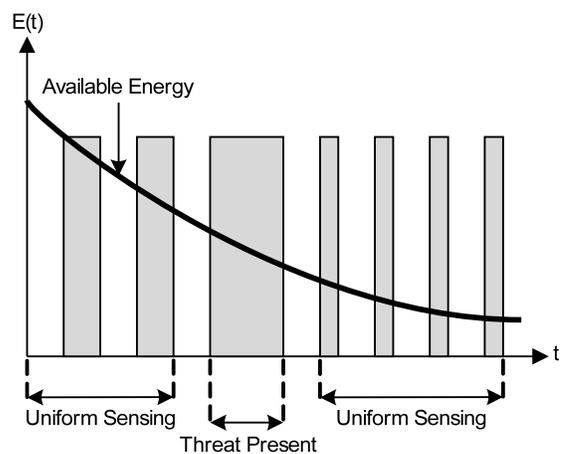


Figure 5: Uniform sensing is performed until a threat is encountered. At this point, T_{active} is extended. Once the threat is out of range, uniform sensing is resumed.

currently available energy, and adjust the length of T_{active} such that uniform sensing can be continued for the remainder of the current cycle. This is clearly illustrated in Figure 5.

A major advantage of the Uniform Sensing Protocol over the static and dynamic active time slot approaches is the fact that uniform sensing does not leave any large openings in the network to be exploited by intruders. In other words, an intruder always has the same chance of being detected, regardless of when it attempts to infiltrate into the network area. This does not hold true for the static and dynamic active period schemes. On the contrary, an intruder has a much higher chance of passing through the network undetected towards the end of the cycle, when most of the sensors have run out of energy, or have drastically reduced their time spent in the active state.

In addition, our protocol is able to adjust to various changes in the environment. For example, if the amount of energy available for harvesting changes due to events such as cloud cover or the nightfall, the sensor nodes will recompute their energy budget taking this into account. Since accurate

Table 1: Simulation Parameters

Parameters	Value	Range
area	$900 \times 600(m^2)$	
number of mobile nodes	1	
number of AFNs	6	
number of coronas	3	
number of wedges	8	
corona width	45 (m)	
number of threat nodes	10	
mobility of threat nodes	1 (m/s)	1-5
number of sensors	200	100-300
sensor transmission range	50 (m)	
sensor sensing range	25 (m)	
max battery capacity	1000 (units)	
discharge rate	5.0 (units/s)	
recharge rate	2.3 (units/s)	
single cycle time	3000 (s)	

intruder tracking is very important, the sensors can extend the length of their active time slot for as long as they sense the intruder’s presence. However, once the threat moves out of the sensing range, the sensor nodes involved will once again adjust their T_{active} to provide uniform sensing. Thus, it is clear that our protocol has significant advantages over the other two approaches. This is confirmed by our simulation results, which are presented in the next section.

4. SIMULATION STUDY

4.1 Simulation environment and metrics

We performed our simulations using the YAES simulator [1], which is a collection of Java libraries that have various sensor network functionalities already implemented in them. In order to perform a quantitative comparison among all three approaches, we considered the following metrics: the average number of failures (mobile node is destroyed by a threat node), average energy consumption by a sensor, and mean time to failure. We varied the number of sensor nodes as well as the mobility of the threat nodes. In our simulations, a random waypoint mobility model was used for the mobile and the threat nodes. Additionally, the speed was kept the same for both types of mobile nodes. Table 1 shows a summary of our simulation parameters and their values.

4.2 Simulation results

The average number of failures is a measure of overall reliability of the network. The goal is to detect all of the existing threats and report their approximate positions, so that the mobile node can avoid them. If the mobile node manages to avoid all of the threats, then the network can be considered reliable. It is obvious that reliability can be improved by adding more sensor nodes.

Figure 6 shows the results of average number of failures versus the number of nodes for all three approaches. It is clear that our protocol generates significantly fewer number of failures than the other two approaches. However, the number of failures tends to decrease with increasing number of nodes for all three schemes, which was expected.

Figure 7 is a summary of simulation results for the average number of failures versus mobility. The number of failures increases with increasing mobility in all three schemes. This

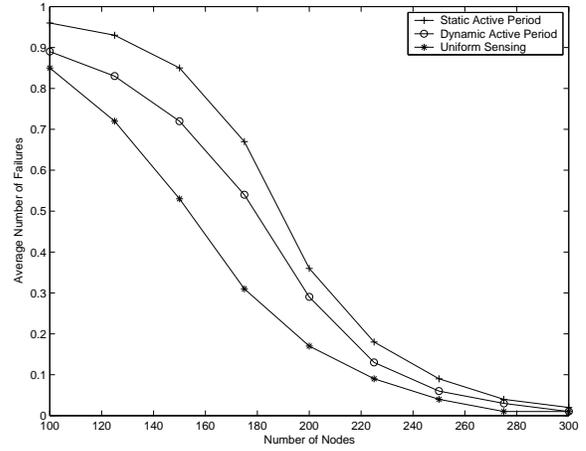


Figure 6: Average number of failures versus the number of sensor nodes.

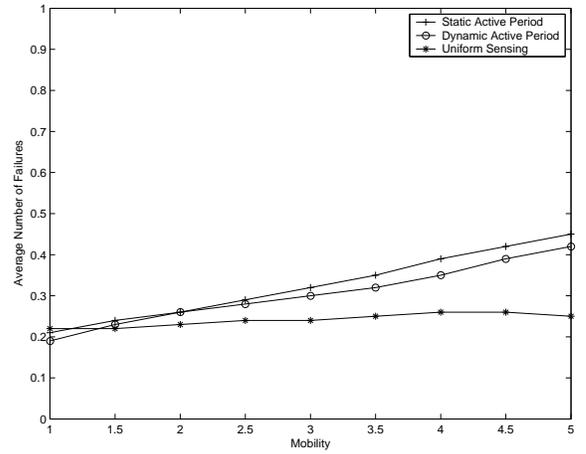


Figure 7: Average number of failures versus mobility.

is due to the fact that it becomes more difficult to track the positions of the threat nodes as they increase their speed. However, the rate at which the number of failures increases is much lower in our protocol than in the other two approaches.

Energy consumption is another measure of network performance. Usually, the goal is to minimize the energy consumption of individual sensor nodes such that the overall lifetime of the network is maximized. However, this is not the case with rechargeable sensors, since energy can be replenished from the environment. Our protocol is specifically designed to *use up* most of the energy in a sensor node. The reasoning behind this is that a sensor should stay active for as long as possible to increase the chances of detecting all of the threats. Thus, the Uniform Sensing Protocol naturally consumes more energy than the other two approaches that we considered.

Figure 8 illustrates the results for the average energy consumption versus the number of nodes. Since the sensing tasks are shared among all of the nodes, the energy consumption of individual sensors tends to decrease with increasing number of nodes. However, the number of nodes

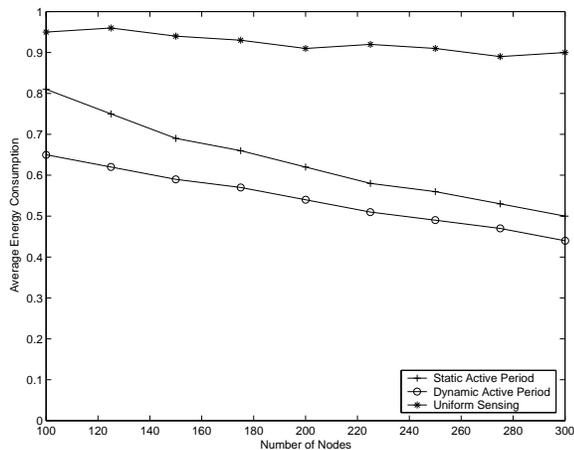


Figure 8: Average energy consumption versus the number of sensor nodes.

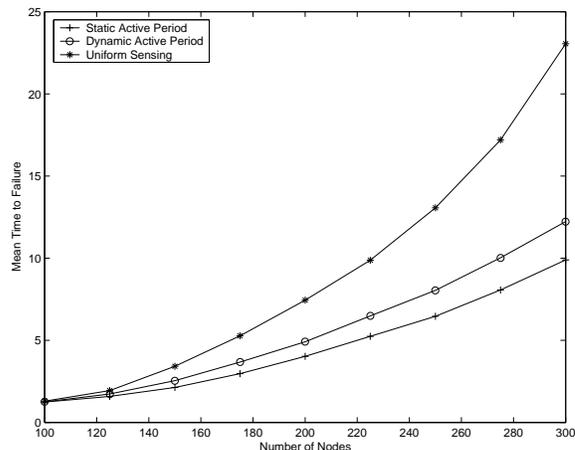


Figure 10: Mean time to failure versus the number of sensor nodes.

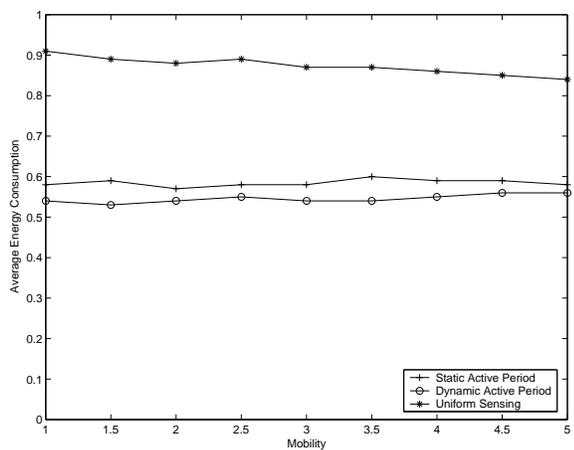


Figure 9: Average energy consumption versus mobility.

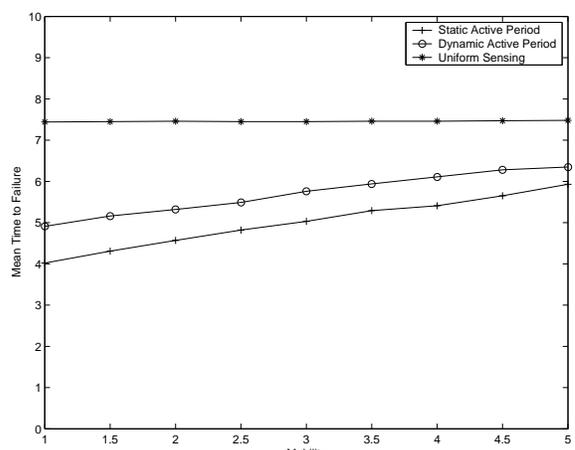


Figure 11: Mean time to failure versus mobility.

seems to have very little effect on the energy consumption under the Uniform Sensing Protocol.

Our simulations show that mobility has no significant impact on the energy consumption of individual sensor nodes, as can be seen in Figure 9. This is due to the fact that energy consumption is based primarily on the available energy in the environment.

Finally, the mean time to failure is also a useful measure of network reliability. The longer a network lasts without having a mobile node being destroyed by the threat nodes, the more reliable a network is. Thus, the main goal is to detect and report the positions of all threat nodes in a timely manner. Our protocol outperformed the other two schemes in this metric as well. Figure 10 clearly shows that the Uniform Sensing Protocol has significantly larger mean time to failure than the static and dynamic active period approaches.

Figure 11 shows a summary of simulation results for the mean time to failure versus mobility. Surprisingly, the static and dynamic active time slot approaches show a slight increase in mean time to failure with increasing mobility. However, our protocol appears to be unaffected by changes in speed of the threat nodes.

The simulation results presented above clearly show that the Uniform Sensing Protocol performs much better than the other two schemes. Specifically, our approach generates on average much fewer failures and has a significantly longer mean time to failure. However, the Uniform Sensing Protocol naturally consumes more energy. Since rechargeable sensors are able to harvest energy from the environment, reliable and timely sensing takes priority over energy conservation in our approach. As a result, the sensor nodes consume most of their energy in a single day and night cycle because their energy supply is likely to be renewed with the coming of day period in the next cycle.

5. CONCLUSIONS

With continuous improvements in micro-electronics and rechargeable technologies, deploying a network that consists entirely of rechargeable sensors is more feasible now than ever before. As a result, there exists a need to exploit the unique characteristics of rechargeable nodes because now efficient energy management becomes somewhat less of an issue, since energy can be harvested from the environment.

In this paper, we propose the Uniform Sensing Protocol for autonomous rechargeable sensor networks. Our approach is unique in the sense that instead of conserving energy consumption by individual nodes, the network tries to use up most of its energy reserves.

Our protocol takes into consideration the amount of available energy in the environment as well as the probability of encountering a certain number of threats. Based on these parameters, each sensor node estimates the length of the active time slot, T_{active} . Once this is accomplished the sensing operations are performed in the usual manner. Additionally, the Uniform Sensing Protocol provides the means of adjusting the length of T_{active} when the amount of available energy in the environment changes, or when a threat is present.

We implemented the Uniform Sensing Protocol, as well as two other protocols, using the YAES simulator [1]. In order to organize the sensor nodes autonomously, we implemented the ANSWER architecture [12]. In our simulations we used the average number of failures, average energy consumption, and the mean time to failure as the simulation metrics. We compared our approach to the static and dynamic active time slot protocols. The simulation results clearly show that the Uniform Sensing Protocol generates fewer failures and has a longer mean time to failure than the other two schemes. Our protocol has naturally higher energy consumption because its focus is on providing uniform and reliable sensing. Efficient energy consumption is a secondary priority, since the nodes can harvest energy from the environment.

6. REFERENCES

- [1] L. Bölöni and D. Turgut. YAES - a modular simulator for mobile networks. In *MSWiM '05: Proceedings of the 8th ACM Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, pages 169–173, October 2005.
- [2] J. Byers and G. Nasser. Utility-based decision-making in wireless sensor networks. In *MobiHoc '00: Proceedings of the 1st ACM International Symposium on Mobile Ad hoc Networking & Computing*, pages 143–144, October 2000.
- [3] J. Hsu, S. Zahedi, A. Kansal, M. B. Srivastava, and V. Raghunathan. Adaptive duty cycling for energy harvesting systems. In *ISLPED '06: Proceedings of the 2006 International Symposium on Low Power Electronics and Design*, pages 180–185, October 2006.
- [4] X. Jiang, J. Polastre, and D. Culler. Perpetual environmentally powered sensor networks. In *IPSN '05: Proceedings of the 4th International Symposium on Information Processing in Sensor Networks*, pages 463–468, April 2005.
- [5] A. Kansal, J. Hsu, M. B. Srivastava, and V. Raghunathan. Harvesting aware power management for sensor networks. In *DAC '06: Proceedings of the 43rd Annual Conference on Design Automation*, pages 651–656, July 2006.
- [6] A. Kansal, J. Hsu, S. Zahedi, and M. B. Srivastava. Power management in energy harvesting sensor networks. *ACM Transactions on Embedded Computing Systems*, 6(4):32, September 2007.
- [7] A. Kansal, D. Potter, and M. B. Srivastava. Performance aware tasking for environmentally powered sensor networks. *SIGMETRICS Performance Evaluation Review*, 32(1):223–234, June 2004.
- [8] A. Kansal and M. B. Srivastava. *Wireless sensor networks: A systems perspective*, chapter 9. Artech House, April 2005.
- [9] K. Kar, A. Krishnamurthy, and N. Jaggi. Dynamic node activation in networks of rechargeable sensors. *IEEE/ACM Transactions on Networking*, 14(1):15–26, February 2006.
- [10] C. Moser, D. Brunelli, L. Thiele, and L. Benini. Lazy scheduling for energy harvesting sensor nodes. In *IFIP International Federation for Information Processing*, volume 225, pages 125–134, 2006.
- [11] A. Nahapetian, P. Lombardo, A. Acquaviva, L. Benini, and M. Sarrafzadeh. Dynamic reconfiguration in sensor networks with regenerative energy sources. In *DATE '07: Proceedings of the Conference on Design, Automation and Test in Europe*, pages 1054–1059, April 2007.
- [12] S. Olariu, M. Eltoweissy, and M. Younis. ANSWER: AutoNomouS netWorked sEnsoR system. *Journal of Parallel and Distributed Computing*, 67(1):111–124, January 2007.
- [13] S. Olariu, A. Wadaa, L. Wilson, and M. Eltoweissy. Wireless sensor networks: leveraging the virtual infrastructure. In *IEEE Network*, pages 51–56, July–August 2004.
- [14] S. Olariu, Q. Xu, and A. Y. Zomaya. An energy-efficient self-organization protocol for wireless sensor networks. In *ISSNIP '04: Proceedings of the Intelligent Sensors, Sensor Networks and Information Processing Conference*, pages 55–60, December 2004.
- [15] J. A. Paradiso and T. Starner. Energy scavenging for mobile and wireless electronics. *IEEE Pervasive Computing*, 4(1):18–27, January–March 2005.
- [16] V. Raghunathan and P. H. Chou. Design and power management of energy harvesting embedded systems. In *ISLPED '06: Proceedings of the International Symposium on Low Power Electronics and Design*, pages 369–374, October 2006.
- [17] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones. Training a wireless sensor network. *Mobile Networks and Applications*, 10(1-2):151–168, February 2005.
- [18] H. Zafar and D. Corkill. Simplifying solar harvesting model-development in situated agents using pre-deployment learning and information sharing. In *ATSN '08: Proceedings of 2nd International Workshop on Agent Technology for Sensor Networks*, pages 41–48, May 2008.
- [19] Y. Zhu and L. M. Ni. Probabilistic wakeup: adaptive duty cycling for energy-efficient event detection. In *MSWiM '07: Proceedings of the 10th ACM Symposium on Modeling, Analysis, and Simulation of Wireless and Mobile Systems*, pages 360–367, October 2007.