Sensor Network Configuration under Physical Attacks

Xun Wang, Wenjun Gu, Kurt Schosek, Sriram Chellappan, Dong Xuan
Department of Computer Science and Engineering,
The Ohio State University, Columbus, OH 43210

***Abstract*— In this paper, we address a sensor network lifetime problem that maintains a certain throughput in an environment where physical node destruction is possible. While lifetime is constrained by limited energy in individual sensors and has been addressed in some detail before, the problem of physical node destruction due to the small form factor and hostile operating conditions of sensors, although significant, has not been addressed before. Specifically, we define a lifetime optimization problem in sensor networks under a representative physical attack model that we define. Our lifetime problem is representative, practical and encompasses other versions of similar problems. Our goal is to derive the minimum number and deployment plan of nodes to meet lifetime requirement. We propose two solutions for this problem. The first solution, *PMR*, deploys nodes only attempting to minimize energy consumption during routing. We show that this approach may not always be optimal. We then propose a second solution, *EPMR*, that deploys nodes *optimally* taking into account the energy minimization and lifetime requirement. We make several observations in this realm. One of our important observations is the high sensitivity of lifetime to physical attacks highlighting the importance of our study. Our work will be important to sensor network designers especially during deployment in hostile terrain.**

Index Terms: System Design, Optimization, Sensor Networks, Physical Attacks.

I. INTRODUCTION

There are many practical applications for wireless sensor networks (WSN) in today's world. These applications range from small, domestic sensor networks that perform indoor climate control, to military applications that detect the presence of chemical agents, to environmental systems that monitor current weather conditions. With improvements in communication ranges, processor/ memory designs, and sensing abilities, the doors have been opened for many new applications employing wireless sensors.

Despite all of the great improvements in other areas, current battery power constraints remain a hurdle to the realization of ubiquitous sensor networks. Sensors can quickly run out of power. This problem is accentuated by the fact that most applications of sensor networks require the sensors to operate in inaccessible environments where, after a one time deployment, recharging or replacing the sensors is not practical. Thus, increasing the operational lifetime of these networks given their limited energy resources has been a major focus of research in the community.

While several works like [1,2,3,4] have proposed bounds on sensor lifetime, works like [5,6] have proposed approaches to maximize useful lifetime of sensor networks. Sensor networks face an additional, albeit significant problem: physical destruction of the sensor nodes. Operation in hostile and uncontrolled environments, coupled with the small size of the sensors and dangers posed by unforeseen calamities (tremors, landslides, falling trees etc), can result in the physical destruction of geographically contiguous nodes. This damage will reduce the overall lifetime of the sensor network. Thus, results on lifetime that have been derived before, although theoretically exciting, have little use in physically hostile environments. The potential for physical destruction of sensor nodes will significantly lower the actual practical lifetime. Thus while the lifetime problem is very important, its practical applicability in the realm of sensor networks is closely intertwined with physical vulnerabilities of the sensor nodes.

In many applications the lifetime of the sensor network is the critical factor. Sensor networks are typically expected to last for a specific duration to sense desired events and the resources have to be procured and deployed to meet the lifetime objective. In this paper, we address the problem of geographically placing sensors in order to attain a desired lifetime under limited sensor energy in an environment where physical destruction of sensors is unavoidable. Our definition of lifetime is the period of time a sensor network can maintain a certain

Manuscript received July 7, 2004. Dong Xuan's work is supported in part by National Science Foundation under grant No. ACI-0329155. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

minimum throughput. Obviously, throughput is a measure of the effectiveness of the sensed data. In achieving desired network objectives, geographical placement of the sensors is critical. In a simple scenario as long as sensors are placed closer to an object of interest, the quality of sensed data is better. Also, from the energy perspective, there is a clear trade-off between few long distance transmissions and many short distance transmissions of the sensed data from the sensors to the base station.

In this paper, the sensor network model we consider is a 2-tier hierarchical model. In this model, sensor nodes are uniformly distributed around the area of interest. Such sensor nodes sense data. A special set of nodes called *Forwarder* nodes (or top tier nodes) collect data from the *Sensor* nodes (or bottom tier nodes) and forward it to a base station. The environment sensed is hostile and uncontrollable resulting in the possibility of attack events that physically destroy a geographically contiguous set of nodes in the vicinity of the attack event. We denote such attacks as *physical attacks*. Such attack events occur frequently and are not isolated. In this scenario, the problem we address is the following: Given a desired time for which the sensor network must maintain a desired minimum throughput of data to the base station, calculate the minimum number of forwarder nodes and determine how they must be deployed in order to achieve the desired objectives when the network is subjected to physical attacks.

We propose two solutions to address this problem. The first is called Power-Minimization Routing based (PMR) solution. Our approach here is to deploy nodes only attempting to minimize energy consumption during routing. While this may be optimal for some cases, we show that this is not always the case. We then propose our second solution, the Enhanced Power-Minimization Routing based (EPMR) solution. The EPMR approach deploys nodes taking into account both energy minimization and lifetime requirement and the resulting solution is *optimal.* In our modeling, we first discuss the case where the sensor network is a circular region. We then discuss extensions where the sensor network can be of any shape.

The lifetime problem we address in this paper is significant. Maintaining a minimum lifetime is a very natural expectation in sensor network applications, and the throughput is a very good measure of the effectiveness of the data transmitted in the network. The physical attack model we define is highly representative of threats in the sensor network environment, which, to the best of our knowledge, has not been addressed in any previous works. In fact, as we demonstrate later, lifetime is indeed sensitive to physical attacks further highlighting the importance of our study. Our paper is organized as follows. In Section II, we present other works related to our study. Section III discusses the problem statement in detail and Section IV provides our solution to the problem. We conduct performance evaluation in Section V, and conclude our work in Section VI.

II. Related Work

In wireless sensor networks there have been a few works on the bounds of lifetime and throughput capacity. In [1], Bhardwaj et al. set forth the upper bound of sensor network lifetime. They argue that transmitting information in the sensor network is the most important limiting factor in network lifetime. They postulate that for any distance D, there is an optimal number of hops of equal length which will minimize the energy needed to transmit data across the entire distance. The length of these equidistant hops is called the characteristic distance (d_{char}). Transmissions that are longer or shorter than the characteristic distance are less energy efficient. Using these minimum energy relays they derive the upper bound for a variety of network scenarios.

While [1] considers only sensor nodes and relay nodes, in [2], Bhardwaj and Chandrakasan extend their previous work to a more sophisticated wireless sensor network which includes aggregator nodes. This work focuses on the upper bound of network lifetime derived by assigning different nodes to be sensor nodes, relays, and aggregators at different times. They apply the concept of minimum energy relays from [1] and then develop an energy efficient collaborative strategy for role assignment. The upper bound of a broad class of wireless sensor networks can be computed using their linear programming algorithm. This class contains the simple pure routing networks, networks that perform both non-hierarchical and constrained hierarchical aggregation, and other dynamic network types, but does not include generalized hierarchical aggregation.

In [3], Hu and Li also focus on the effects that energy constraints have on the lifetime of wireless sensor networks. This work defines the operational lifetime of the network in terms of both energy consumption and network throughput. They specifically study the effect of node density on the network operational lifetime and determine the maximum sustainable throughput given the energy constraints in a typical wireless sensor network. While the above works discuss the problem of bounding lifetime in sensor networks, we address a more practical deployment problem that achieves desired lifetime objectives.

Some work has also been done in the area of node placement relative to target detection. In [7] Chakrabarty

et al. provide an algorithm that allows the determination of node placement on a grid in order to provide coverage of a certain target area. Their main problem is to distribute nodes of differing sensing power, and therefore monetary cost, in such a way that the area is covered with minimal cost. On the other hand, Clouqueur et al. propose an algorithm in [8] to determine a deployment strategy given that only the number and density of nodes in an area can be determined a priori. They develop the concept of path exposure, or the probability that a target moving in the sensor network will be detected, and then use simulation to determine the statistical distribution of exposure for the placement of a certain number of nodes. Based on this information a network designer can deploy a certain number of nodes, observe the node deployment and then determine if additional nodes must be deployed to achieve acceptable exposure.

While our work has similarities with the previous works, we study the problem under the presence of physical attacks. Randomness due to the nature of such attacks makes our problem even more difficult. We incorporate throughput, forwarding, and energy constraint and attack parameters in order to more realistically model a wireless sensor network.

Many sensor networks will be deployed in hostile environments. These environments can be physically hostile where physical destruction of sensor nodes is an important problem that cannot be ignored. It is in fact an issue of sensor network security, especially if physical destruction can be orchestrated by an attacker. In terms of sensor network security, Karlof and Wagner explore sensor network routing protocol vulnerability and reaction to several electronic attacks [9]. They consider many common routing protocols, document their vulnerability to various attacks, and propose countermeasures and design principles for securing these, and future, protocols. Most recently, Wood and Stankovic discussed various denial of service attacks that can be directed against wireless sensor networks [10]. They describe the threats at the various levels of the protocol stack and posit wireless sensor network design principles to counter these threats.

III. System Model And Problem Setup

We address an optimization problem in this paper where we determine an optimal number and deployment of nodes that ensures a desired lifetime in a sensor network sustaining a minimum throughput. The environment is one where hostile events can physically destroy the nodes.

In the following, we first define our sensor network model and attack model followed by the actual definition of the problem we study. All notations, their definitions and standard values used in this section and in the rest of the paper are given in Table I. Empty fields in Column 3 of Table I imply that the corresponding parameters are variables that are used in performance evaluation.

A. Sensor Network Model

The sensor network environment (or sensor field) we study consists of n^s sensor nodes uniformly deployed over a circular area of radius D. The area of the sensor network is then $\pi \cdot D^2$. Each sensor node initially has e^s joules of energy. The sensor nodes continuously transmit data at a rate r towards a base station (BS)

TABLE I. NOTATIONS, DEFINITIONS AND STANDARD VALUES

Notation	Definition	Value
α_1	Receiver constant	180nJ/bit
α_2	Transmitter constant	10pJ/bit/m2
n	Path loss factor	2
e^s	Initial power of sensor node[a]	2200J
e^f	Initial power of forwarder node[b]	18400J
r	The sending rate	2kbps
d_{char}	Characteristic distance	134.16 meters
T	Desired lifetime	
$C(0)$	Initial throughput	n^s *r
$C(t)$	Throughput at time t	
C^*	Desired throughput	
λ	Attack arrival rate	
A	The radius of the area destroyed per attack instance	
n^s	Number of sensor nodes	
n^f	Number of forwarder nodes	
β_d	Density of forwarder nodes at distance d from BS	
D	Sensor network radius	
cf	Confidence interval	

located at the center of the sensor field as shown in Fig. 1. In our radio model [1], the power expended in relaying (receiving then transmitting) a traffic flow with data rate r to a receiver located at distance d is given by

[a] Initial power for sensor node is based on 500mA-hr, 1.3V battery.
[b] Initial power for forwarding node is based on 1700mA-hr, 3V battery which is similar to the PicoNodes used in [11].

$$\overline{p(d)} = r(\alpha_1 + \alpha_2 d^n). \quad (1)$$

Assuming a $1/d^n$ path loss [1], α_1 includes the energy/bit consumed by the transmitter electronics (including energy costs of imperfect duty cycling due to finite startup time) and the energy/bit consumed by the receiver electronics, and α_2 accounts for energy dissipated in the transmit op-amp (including op-amp inefficiencies). Standard values of α_1, α_2, n are given in Table I.

Sensor nodes use a set of nodes called *forwarder nodes* as relays to transmit their data to the BS. The forwarder nodes do not generate data. That is, their purpose is only to forward the traffic from the sensor nodes to an appropriate forwarder node. The data is then relayed using other forwarder nodes located progressively closer to the BS. The data transmission from a sensor node to its nearest forwarder node is one hop, while the data from the forwarder node to the BS requires one hop or many hops through other forwarder nodes to the BS. Forwarder nodes can increase their transmission range at the cost of more energy dissipation according to (1). Each forwarder node initially has e^f joules of energy.

B. Attack Model

Sensor networks are typically expected to operate in hostile terrain and environments. This fact, coupled with the node's small form factor, make the sensor and forwarder nodes very susceptible to physical destruction. Towards this end of describing physical attacks, our first step is to develop a suitable attack model that is representative of the physical network structure and mathematically tractable.

In this paper we define a novel and highly representative physical attack model as follows: Attack events occur in the sensor field of interest. Each event destroys an area in the field. Nodes (sensor nodes and forwarder nodes) located within this area are physically destroyed. To give an example, if attack events follow a Poisson distribution, then the probability of k attacks in a time interval t, with a mean arrival rate λ is given by

$$\Pr[N = k] = \frac{e^{\lambda \cdot t} \cdot (\lambda \cdot t)^k}{k!}.$$

In this paper, we assume that the attack area is a circular region and is a constant for all attacks. Thus for an attack radius A, the area destroyed is $\pi \cdot A^2$. The attack events are assumed to be uniformly geographically distributed over the sensor field. We assume that the BS will not be destroyed during attacks.

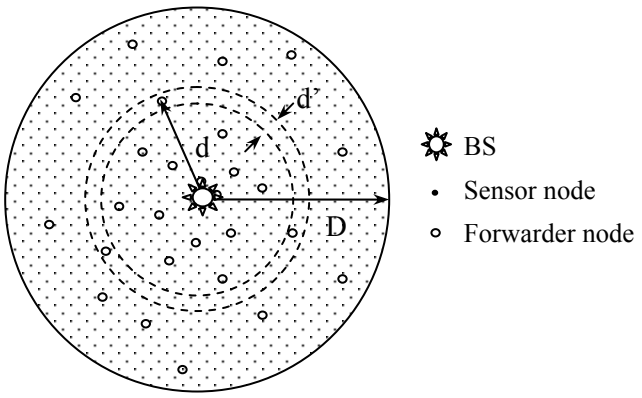

Figure 1. A uniformly distributed sensor network with BS at the center of the network.

C. Problem Setup

In the following, we define a scenario where, the sensor network is a circular region of radius, D. Attack events occur following a Poisson distribution with rate λ and are uniformly geographically distributed. Attack events destroy a circular region of radius, A. Sensor nodes continuously transmit data to the BS using Forwarder nodes as relays. The effectiveness of the sensor network is measured by the overall throughput received by the BS. It is quantified by the amount of bits received per second.

In this scenario we address the following problem: Given a sensor network consisting of n^s uniformly distributed sensor nodes that continuously send data to a BS (refer to Fig. 1), and given a desired lifetime T for which the network must maintain a minimum throughput C^* with a confidence, cf, determine the minimum number of forwarder nodes n^f and the optimal geographical deployment of these nodes in the sensor field such that the lifetime is guaranteed under physical attacks. More specifically, we wish to calculate the optimal number of the forwarder nodes at distance d away from the BS. We denote this number as β_d. The forwarder nodes in β_d are distributed uniformly in a ring at a distance d from the BS. In this case, d ranges between $(0, D)$, where D is the radius of the sensor field. The integration of β_d is the total number of needed forwarder nodes, n^f. We formally define our problem in Fig. 2. In this paper we first study the case where the sensor network is a circular field. We also discuss extensions to a general topology.

D. Discussion

Our objective in this paper is to solve an optimization problem. We do not consider the effects of channel assignments, decisions, collisions between simultaneous communications, etc. In this sense our work can also be considered an upper bound on the attainable lifetime if the forwarder nodes are deployed according to the criteria in this paper. Other versions of this problem also exist. For instance, for a given set of forwarder node resources, what is the maximum attainable lifetime? The problem we address however is important. First, network lifetime is a serious concern for most sensor network applications. Such applications typically require sensor nodes to be operational for a desired time.

As such, the problem we address is very practical and of immediate use to the system designer. Second, other versions of this problem can be readily addressed based on our solution to this problem. For instance, if the maximum possible lifetime needs to be calculated for a given set of forwarder nodes, application of our approach and a simple binary search will yield the desired results. Third, our analysis includes the presence of physical attacks.

IV. Problem Solution

A. Overview

In the 2-tier sensor network that we consider, the problem we address is the number and deployment of the forwarder nodes. Intuitively we should deploy forwarder nodes keeping in mind several constraints covered in the following paragraphs.

The forwarder nodes towards the BS receive more traffic than those progressively away from the BS. That is, there is a convergence of traffic at nodes nearer to the BS. To compensate for this disparity in traffic reception and to make the energy dissipation geographically uniform, the density of forwarder nodes should progressively increase towards the BS. However the presence of physical attacks could destroy a contiguous portion of nodes introducing some new challenges addressed below.

Input:

System Side: n^s, D, r, C^*, T, cf, e^s, e^f

Attack side: , λ, A

Objective:

Achieve desired lifetime with minimum number of forwarder nodes.

Output:

n^f, β_d

Figure 2. Problem definition.

We solve a deployment problem in this paper. The output of our solution is not just the number of forwarder nodes but also a detailed deployment plan for those nodes. The deployment plan will show how many forwarder nodes to deploy where. We use the density of forwarder nodes to quantify the deployment. It is easy to see that the density depends on the distance to the BS. Recall that we denote the density of forwarder nodes at a distance d away from the BS as β_d. Once the problem is solved, a list of β_d for different d will be obtained. The integration of β_d is the total number of needed forwarder nodes.

To solve our problem, we need to derive the formulas to compute the total traffic throughput to the BS and the power consumption of each forwarder node. In the following subsections describe our derivation of a mathematical model of these two requirements and then present our solution to the overall problem.

B. Throughput and Power Consumption Rate Computation

In this subsection, we discuss how to compute the sensor network throughput and then describe the derivation of the power consumption rate for each forwarder node. The definitions for notations used here are provided in Table I.

1) Computing the sensor network throughput

The sensor network throughput, $C(t)$, changes over time. To compute $C(t)$, we need to know the total number of sensor nodes which send traffic to the BS. We use a two pronged approach. We first calculate the number of sensor nodes in the absence of physical attacks and then in the presence of attacks.

With the above classification of sensor nodes, the number of sensor nodes whose traffic can reach the BS without considering physical attacks is:

$$S(t) = \alpha \cdot \int_{u=0}^{d_{\min}} 2 \cdot \pi \cdot u \cdot \prod_{i=1}^{H(u)} f^{f}_{u-\sum_{k=1}^{i} d_m(k,u,t)}(t) \cdot du. \qquad (2)$$

In (2), α is the density of the sensor nodes. In our network, there are n^s sensor nodes uniformly distributed in the area of the size πD^2. α is given by,

$$\alpha = \frac{n^s}{\pi \cdot D^2}. \qquad (3)$$

Here $2 \cdot \alpha \cdot \pi \cdot u \cdot du$ is the number of sensor nodes that are at a distance u away from the BS. In order to guarantee transmission to the BS, all forwarder nodes in its path to the BS need to be alive. This is quantified by $\prod_{i=1}^{H(u)} f^{f}_{u-\sum_{k=1}^{i} d_m(k,u,t)}(t)$ (More explanation for this follows.)

In order to calculate $\prod_{i=1}^{H(u)} f^{f}_{u-\sum_{k=1}^{i} d_m(k,u,t)}(t)$, we need $d_m(k,u,t)$, $H(u)$ and $f_u^f(t)$. The average hop routing distance of the k^{th} hop for the sensor nodes that are at a distance u away from the BS at time t is denoted as $d_m(k,u,t)$. This value depends on the routing policy, which will be discussed in the next subsection.

We denote $H(u)$ as the number of forwarder nodes needed by a sensor node that are at a distance u away from the BS at time t to send traffic to the BS. $H(u)$ is the value that satisfies both of the following inequalities, (4) and (5), below.

$$u - \sum_{k=1}^{H(u)+1} d_m(k,u,t) \le 0 \tag{4}$$

$$u - \sum_{k=1}^{H(u)} d_m(k,u,t) > 0 \tag{5}$$

We denote $f_u^f(t)$ as an indicator that shows whether the forwarder nodes u distance away from the BS are out of power (with value 0) or are active (with value 1) at time t. It is given by,

$$f_u^f(t) = \begin{cases} 0, & where \int_{s=0}^{t} p_u^f(s)ds \ge e^f \\ 1, & where \int_{s=0}^{t} p_u^f(s)ds < e^f. \end{cases} \tag{6}$$

We denote the power consumption rate for a forwarder node at a distance u away from the BS at time t with the notation $p_u^f(t)$.

In (2), d_{min} is the radius of the area centered at the BS within which the traffic from the sensor nodes is required to be forwarded to guarantee the throughput requirement. In some cases d_{min} is less than D, for instance, where the required throughput C^* is relatively small compared to the total amount of traffic from the sensor nodes. In this case it is not necessary to deploy forwarder nodes in order to cover all sensor nodes since the objective of this problem is minimizing the number of forwarder nodes.

We now compute the number of sensor nodes, $S^*(t)$, that can successfully forward traffic to the BS under physical attacks. Before actually proceeding with its derivation, we discuss necessary attack preliminaries.

Due to the randomness of the attack arrival, our problem is guaranteeing lifetime with a confidence, say cf. This confidence is captured by the number of attack events expected to arrive as discussed below.

We denote $m(t)$ as the number of physical attacks that are expected to arrive in a time period t. With a confidence interval cf, $m(t)$ is calculated from,

$$\sum_{i=0}^{m(t)-1} \Pr(N=i,t) < cf \text{ and } \sum_{i=0}^{m(t)} \Pr(N=i,t) \ge cf, \tag{7}$$

in which $\Pr(N=i,t)$ is the probability that the number of physical attacks during time t is i. If the physical attack follows Poisson distribution, $\Pr(N=i,t)$ is given by $e^{-\lambda \cdot t} \cdot (\lambda \cdot t)^i / i!$.

It is easy to see that $(\pi \cdot D^2 - \pi \cdot A^2)/(\pi \cdot D^2)$ is the ratio of remaining sensor or forwarder nodes to the total initial number of sensor or forwarder nodes after one instance of physical attack. We assume that the physical attacks are independent, so the ratio of remaining sensor or forwarder nodes after $m(t)$ physical attacks is $[(\pi \cdot D^2 - \pi \cdot A^2)/(\pi \cdot D^2)]^{m(t)}$. Hence, the number of sensor nodes whose traffic can reach the BS under physical attacks is:

$$S^*(t) = \alpha \cdot \int_{u=0}^{d_{\min}} 2 \cdot \pi \cdot u \cdot \prod_{i=1}^{H(u)} f^{f}_{u-\sum_{k=1}^{i} d_m(k,u,t)}(t) \cdot du \cdot \left(\frac{\pi \cdot D^2 - \pi \cdot A^2}{\pi \cdot D^2} \right)^{m(t)}. \tag{8}$$

It is now simple to calculate the overall network throughput. Hence, the network throughput at time t is $S^*(t) \cdot r$, where r is the sending rate of the sensor nodes. Thus the throughput in the sensor network subject to physical attacks is given by,

$$C(t) = \int_{u=0}^{d_{\min}} 2 \cdot \pi \cdot u \cdot \prod_{i=1}^{H(u)} f^{f}_{u-\sum_{k=1}^{i} d_m(k,u,t)}(t) \cdot du \cdot \alpha \cdot \left(\frac{\pi \cdot D^2 - \pi \cdot A^2}{\pi \cdot D^2} \right)^{m(t)} \cdot r. \tag{9}$$

2) Computing the power consumption rate

In this subsection, we discuss how to compute the power consumption rate for each forwarder node. The power consumption rate changes over time and each forwarder node has a different power consumption rate. However, the sensor network we are studying is a circle, the BS is at the center of the network, and the sensor nodes are uniformly distributed throughout the network area. We can thus claim that forwarder nodes with the same distance to the BS have the same power consumption rate. We denote the power consumption rate for a forwarder node at a distance d away from the BS at time t as $p_d^f(t)$.

To compute $p_d^f(t)$ we need to compute the traffic forwarding rate of each node d away from the BS and

the next hop distance. This next hop may be another forwarder node or the BS.

We introduce the concept of region here to compute $p_d^f(t)$. A region covers an area between $d - d'/2$ and $d + d'/2$, where d is the distance from the BS (refer to Fig. 1). Its width is d'. Here we discuss the case where the forwarder node is at least $d_m(1,d,t)$ away from the BS. In this case, the forwarder node needs to find another forwarder node to forward the traffic. We then have,

$$d' = d_m(1,d,t). \tag{10}$$

We will discuss the case where the distance of the forwarder node from the BS is less than $d_m(1,d,t)$ later.

We define u' as $d + d'/2$. The total amount of traffic from the sensor nodes whose distances from the BS are between u' and d_{min} under physical attacks is given by

$$l_d^f(t) = \int_{u=u'}^{d\min} 2\cdot\pi\cdot u\cdot du\cdot\alpha\cdot\left(\frac{D^2-A^2}{D^2}\right)^{m(t)}\cdot r. \tag{11}$$

This traffic will be forwarded by the forwarder nodes in this region once and only once since the width of this region is d', i.e. $d_m(1,d,t)$. Hence $l_d^f(t)$ represents the total traffic amount which the forwarder nodes in this region need to forward.

To compute the traffic load to a single forwarder node, we need to obtain the total number of forwarder nodes $n_d^f(t)$ in this region, given by

$$n_d^f(t) = \int_{u=d-d'/2}^{u=d+d'/2} 2\cdot\pi\cdot u\cdot\beta_u\cdot\left(\frac{D^2-A^2}{D^2}\right)^{m(t)} du. \tag{12}$$

We assume that the traffic load is uniformly distributed among all forwarder nodes in this region. Hence, the traffic load to a forwarder node at distance d and time t, denoted by $w_d^f(t)$, is given by $l_d^f(t)/n_d^f(t)$. That is,

$$w_d^f(t) = \frac{\int_{u=u'}^{d\min} 2\cdot\pi\cdot u\cdot f_u^s(t)\cdot du\cdot\alpha\cdot\left(\frac{D^2-A^2}{D^2}\right)^{m(t)}\cdot r}{\int_{u=d-d'/2}^{u=d+d'/2} 2\cdot\pi\cdot u\cdot\beta_u\cdot\left(\frac{D^2-A^2}{D^2}\right)^{m(t)}\cdot du}. \tag{13}$$

Having obtained the traffic load to a forwarder node, we need to compute the routing distance of the forwarder node to forward the traffic to the next hop. For the forwarder nodes whose distance from the BS, *d,* is less than $d_m(1,d,t)$, their next transmission distance is always *d*. However, for other nodes, it is not guaranteed that each forwarder node in the region can find the next hop forwarder node with a distance of exactly $d_m(1,d,t)$, which is d'. The range of the routing distance will be between $d'/2$ and $3\cdot d'/2$. We assume that the next hop distances are uniformly distributed in this interval. Therefore, the distribution function *Pr(u)* of routing distance of the forwarder nodes that are at a distance u away from the BS is given by

$$\Pr(u) = \begin{cases} 1/d', & where\ d > d' \\ 1, & where\ d \le d', u = d \\ 0, & where\ d \le d', u \ne d. \end{cases} \tag{14}$$

The average power consumption rate to relay one bit of data for a forwarder node that is at a distance *d* away from the BS at time *t* is given by

$$\bar{p}_d^f(t) = \int_{u=d'/2}^{3\cdot d'/2} (\alpha_1 + \alpha_2 u^n)\cdot\Pr(u)\cdot du. \tag{15}$$

Thus the power consumption rate of a forwarder node at a distance *d* away from the BS at time *t* is $w_d^f(t)\cdot\bar{p}_d^f(t)$, or

$$p_d^f(t) = \frac{\int_{u=u'}^{d\min} 2\cdot\pi\cdot u\cdot du\cdot\alpha\cdot\left(\frac{D^2-A^2}{D^2}\right)^{m(t)}\cdot r}{\int_{u=d-d'/2}^{u=d+d'/2} 2\cdot\pi\cdot u\cdot\beta_u\cdot\left(\frac{D^2-A^2}{D^2}\right)^{m(t)}\cdot du \cdot\int_{u=d'/2}^{3\cdot d'/2}(\alpha_1+\alpha_2 u^n)\cdot\Pr(u)\cdot du.} \tag{16}$$

The above formula can be simplified to

$$p_d^f(t) = \frac{[d_{\min}^2 - (d + d_m(1,d,t)/2)^2]\cdot\alpha\cdot r}{2\cdot d\cdot d_m(1,d,t)\cdot\beta_d \cdot\int_{u=d'/2}^{3\cdot d'/2}(\alpha_1+\alpha_2 u^n)\cdot\frac{1}{d'}\cdot du.} \tag{17}$$

The case we study above considers when the distance of the forwarder node from the BS is at least $d_m(1,d,t)$. Now we extend the above formula to the case that $d < d_m(1,d,t)$. In this case, d' is *d*. Thus $p_d^f(t)$ can be given by the following general formula:

$$p_d^f(t) = \begin{cases} \dfrac{[d_{\min}^2 - (d + d_m(1,d,t)/2)^2]\cdot\alpha\cdot r}{2\cdot d\cdot d_m(1,d,t)\cdot\beta_d} \cdot\int_{u=d'/2}^{3\cdot d'/2}(\alpha_1+\alpha_2 u^n)\cdot\dfrac{1}{d'}\cdot du, \\ \qquad where\ d \ge d_m(1,d,t)\ \ and \\ \dfrac{[d_{\min}^2 - (d_m(1,d,t))^2]\cdot\alpha\cdot r}{2\cdot d^2\cdot\beta_d}\cdot(\alpha_1+\alpha_2 d^n), \\ \qquad wherre\ d < d_m(1,d,t). \end{cases} \tag{18}$$

The overall power consumption of a forwarder node that is at a distance *d* away from the BS is given by $\int_{t=0}^{T} p_d^f(t)\cdot dt$. The total number of forwarder nodes in the sensor network can be calculated by,

$$n^f = \int_{u=0}^{D} 2\cdot\pi\cdot u\cdot\beta_d\cdot du \tag{19}$$

C. Our Solution

Having derived the formulas to compute *C(t)* and $p_d^f(t)$, our problem can be expressed as described in Figure 3. We propose two solutions to this problem. The first one is called the Power-Minimization Routing based solution, *PMR*, and the second is an enhanced version of the *PMR* solution, or the Enhanced-Power-Minimization Routing based solution, *EPMR*, solution.

Objective: Minimize n^f

Constraints:

$\int_{t=0}^{T} p_d^f(t) \cdot dt \le e^f$ (20), $p_d^f(t)$ is given in (18)

$$C(t) = \int_{u=0}^{d_{\min}} 2 \cdot \pi \cdot u \cdot \prod_{i=1}^{H(u)} f^{f}_{u-\sum_{k=1}^{i} d_m(k,u,t)}(t) \cdot du \cdot \alpha \cdot \left(\frac{\pi \cdot D^2 - \pi \cdot A^2}{\pi \cdot D^2} \right)^{m(t)} \cdot r \ge C^* \quad (21)$$

Figure 3. Restated problem description.

1) The Power-Minimization Routing Based (PMR) Solution

The main idea of this solution is to deploy forwarder nodes in such way that the forwarder energy spent in the whole system is minimized and the total number of nodes minimized.

Energy consumption is determined by the routing policy. The routing policy includes the number of intermediate forwarder nodes and the transmission distance. In [1], if each forwarder node's transmission distance is equal to the d_{char} shown in (22), the energy consumption is minimum. In (22), α_1, α_2, and n are the receive, transmit amplifier, and path loss constants.

$$d_{char} = \sqrt[n]{\frac{\alpha_1}{\alpha_2 (n-1)}} \quad (22)$$

Hence we can deploy forwarder nodes in such way that each forwarder node can always find the next forwarder node in d_{char} during the entire lifetime.

To guarantee a routing distance of d_{char}, a certain density of forwarder nodes needs to be deployed so that the average distance between two neighboring forwarder nodes towards the BS, $\underline{d}$, should be less than or equal to d_{char}. In this sense, the density of forwarder nodes is important to maintain the efficiency of routing. In order to achieve optimal routing, traffic load should be distributed among the forwarder nodes so that none of the forwarder nodes run out of power before the desired lifetime is achieved. With this arrangement, the density of the forwarder nodes will not change because of power consumption. Therefore, the routing efficiency will not depend on forwarder node power consumption.

We denote the function mapping the network forwarder node density β and $\underline{d}$ *G(.)*. A reasonable *G(.)* is $\underline{d} = \sqrt{1/\beta}$ or $\beta = 1/\underline{d}^2$. We denote the network density which can guarantee d_{char} as β_{char}. In order to guarantee d_{char} under physical attack over a time period *t*, the initial node density β_{char} should be greater than or equal to $1/(d_{char}^2 \cdot (\frac{\pi \cdot D^2}{\pi \cdot D^2 - \pi \cdot A^2})^{m(t)})$.

With the above routing arrangement, enough forwarder nodes will be available for routing through the entire lifetime to guarantee d_{char}. Formula (21) can be simplified as follows

$$C(t) = \pi \cdot d_{\min}^2 \cdot \alpha \cdot \left(\frac{D^2 - A^2}{D^2} \right)^{m(t)} \cdot r \ge C^*. \quad (23)$$

We can determine the density of forwarder nodes based on the requirement of routing over a distance of d_{char}. In order to meet the lifetime requirement under attack, assuming the routing distance d_{char}, we can also derive another minimum network density requirement, denoted as β_d^{power}. β_d^{power} can be computed from (18), (20) and (23) as follows:

Given the routing distance is always d_{char}, $d_m(k,u,t)$, the average routing distance of the first next hop, is d_{char}. Once $d_m(k,u,t)$ is determined, d_{min} can be calculated based on (23), and then β_d^{power} can be computed from (18) and (20). Note that in general cases d_{min} is less than *D*, the radius of the sensor network. However, in special cases, where, for instance, *C** is so big that the number of present sensor nodes cannot provide enough traffic, d_{min} is larger than *D*. Under this situation, the network is not deployable.

Once we get both β_{char} and β_d^{power}, our *PMR* solution is to calculate the maximum of these two variables, i.e. $\beta^{PMR} = \max(\beta_{char}, \beta_d^{power})$. Under β_d^{PMR}, the routing distance can always be guaranteed to be d_{char}, and the life time requirement can also be satisfied under attack.

We need to consider the constraints of e^s on our result. In order to make e^s last over the lifetime *T*, the maximum transmission distance of the sensor node to a forwarder node is $d_s = \sqrt[n]{(e^s/(T \cdot r) - \alpha_1)/(\alpha_2 \cdot (n-1))}$. We should deploy the forwarder nodes in such a way that the source nodes can always find a forwarder node in a distance less than d_s. From this we can derive a lower bound of β_d, denoted by β_s. With the function mapping the network forwarder node density β and $\underline{d}$ *G(.)*, $\beta = 1/\underline{d}^2$, we can derive the lower bound constrained by e^s, i.e. $\beta_s = 1/d_s^2$. Considering this bound, with the PMR solution, β^{PMR} should be $\max(\beta_{char}, \beta_d^{power}, \beta s)$.

2) The Enhanced Power-Minimization Routing Based (EPMR) Solution

By carefully studying the two basic requirements of the above solution, we find that the lifetime requirement is a necessary requirement. According to the definition of our problem, this requirement must be satisfied. Deploying nodes with a density of β_d^{power} guarantees the minimum required power in order to meet the lifetime requirement. It thus provides a lower bound on the network density. However recall that in computing β_d^{power}, we assume optimal routing distance (d_{char}). This is guaranteed with a deployment density of β_{char}. With the PMR solution, if $\beta_{char} \leq \beta_d^{power}$, then β^{PMR} is equal to β_d^{power}. Deployment with a density of β_d^{PMR} satisfies the lifetime requirement, while ensuring minimum energy during routing. Thus β_d^{PMR} is optimal.

However, if $\beta_{char} > \beta_d^{power}$, can the PMR solution always get the optimal result? The answer is no. Consider a simple case where each forwarder node has a lot of power to handle all forwarding tasks. In this case only a few or even one forwarder node is enough to meet the lifetime requirement. This in turn means that the density of forwarder nodes is extremely small and routing distance need not necessarily be d_{char} and optimal energy routing is not necessary here.

Based on the above considerations, we propose our second solution, EPMR, which is an enhancement of the PMR solution. In the PMR solution, if $\beta_{char} > \beta_d^{power}$, the node density will be decided by β_{char}. This means more forwarder nodes than the necessary ones based on (18), (20) and (23) will be deployed. But our objective here is to guarantee only the lifetime with a minimum number of forwarder nodes. Hence, in EPMR we do not deploy nodes with the intention of guaranteeing β_{char}. Instead we only need to deploy minimal number of nodes to meet the lifetime requirement. However, if we decrease the density to be smaller than β_{char}, d_{char} cannot be guaranteed, and optimum energy routing cannot be achieved. Consequently, β_d^{power}, which is calculated assuming a routing distance of d_{char}, may need to be increased due to the actual hop distance being bigger than d_{char}. In order to get the optimum, i.e. the optimal nodes density β_d (and the corresponding hop distance) at the distance d away from the BS, we design an iterative procedure to get the minimum density which can satisfy (18), (20) and (23). Thus we obtain the optimum lying between β_{char} , which gives an upper bound and β_d^{power} , which gives the lower bound of the network density when $\beta_{char} > \beta_d^{power}$. Regarding βs, the EPMR solution uses a similar method to consider it with the *PMR* solution.

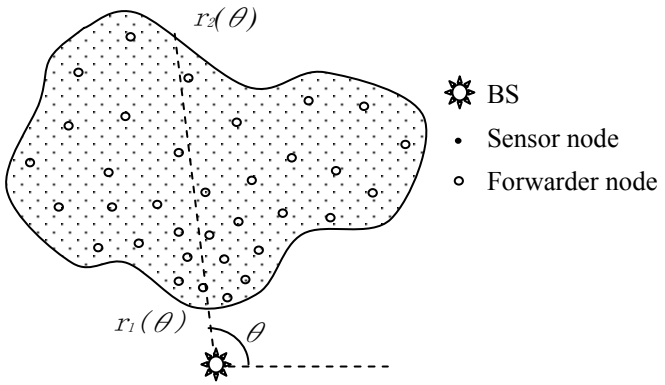

Figure 4. General sensor network topology.

With the EPMR solution, the routing distance cannot be always guaranteed to be d_{char}. In fact,

$$d_m(1,u,t) = \max(d_{ch}(u,t), d_{char}), \qquad (24)$$

where $d_{ch}(u,t)$ is the actual average one hop distance for node that is at a distance u away from the BS at time t, which is given by $d_{ch}(u,t) = \sqrt{1/\beta_u(t)}$ (according to $G(.)$). Here $\beta_u(t)$ stands for the forwarder nodes density in the area that is at a distance u away from the BS at time t. The density at initial time is $\beta_u(0) = \beta_u$.

D. Extension

In this subsection, we want to discuss the extension to our work. The network in our problem is a circular region with the BS at the center of the network. Many sensor networks have a generally amorphous shape with the base station in a location other than the center of the network. In such networks, the assumption that the traffic load is uniformly distributed among forwarder nodes no longer holds. However, our method can be extended as follows.

Imagine using polar coordinates to describe the area as shown in Fig. 4. With the BS as the Pole, the distance from any point on the boundary of the area can be described as $r(\theta)$, where r is the distance from the BS and θ is the polar angle for that point. The general formula to calculate $C(t)$ is given by,

$$C(t) = \int_{\theta=0}^{2\pi} \left(\int_{u=r_1(\theta)}^{r_2(\theta)} u \cdot \prod_{i=1}^{H'(u)} f^{f}_{u-\sum_{k=1}^{i} d_m(k,u,t)}(t) du \right) \cdot \alpha \cdot r \cdot R^{m(t)} d\theta, \quad (25)$$

in which, $H'(u)$ is the value which satisfies

$$u - \sum_{k=1}^{H'(u)+1} d_m(k,u,t) \le r_1(\theta) \text{ and } u - \sum_{k=1}^{H'(u)} d_m(k,u,t) > r_1(\theta),$$

where R is $(\pi \cdot D^2 - \pi \cdot A^2)/(\pi \cdot D^2)$.

Note that there can be two points on the boundary with the same angle θ. We then denote $r_1(\theta) \le r_2(\theta)$.

Then $p_d^f(t)$ needs to be extended as $p_d^f(\theta,t)$, because the forwarder nodes having the same distance from the BS now may have different traffic overhead. The power consumption rate now should also depend on the polar angle, not just the distance from the BS *(d)* and time (*t*). The power consumption rate of a node d away from the BS with polar angle θ at time t is

$$p_d^f(\theta,t) = \frac{\int_{u=u''}^{r(\theta)} u \cdot du \cdot \alpha \cdot R^{m(t)}}{\int_{u=d-d''/2}^{u=d+d''/2} u \cdot \beta_u \cdot R^{m(t)} \cdot du} \cdot \int_{u=d''/2}^{3\cdot d''/2} \overline{p(u)} \cdot Pr(u) \cdot du, \quad (26)$$

in which d'' can be given by,

$$d'' = \begin{cases} d, & where\ d \le r_1(\theta) + d_m(1,d,t) \\ d_m(1,d,t), & where\ d > r_1(\theta) + d_m(1,d,t) \end{cases}$$

Having derived $C(t)$ and $p_d^f(\theta,t)$, we can still apply our proposed solutions, i.e. PMR and EPMR, to solve the original problem with a general sensor network topology.

V. Performance Evaluation

In this section, we report our performance data based on the analysis in Section IV. Our motivation is to compare the performance of the PRM and EPRM solutions in optimizing the number of forwarding nodes. We also wish to study the impacts of physical attacks on the sensor network configuration. Our sensor network is a circular region of radius, D. The BS is located at the center of the field. Attack events follow a Poisson distribution with a rateλ. Each event destroys a circular region of radius A. The attacks are uniformly geographically distributed. Table I in Section III lists some of the fixed parameters for the sensor nodes and the sensor network environment. Table II, below, lists the parameters we have used for the physical attack and lifetime requirement. The desired throughput C^* is set at *60%* of the initial throughput *C(0)*.

We use MATLAB to get the performance data based on the formulas derived in Section IV.

Fig. 5 shows the performance improvement of the EPMR solution over the PMR approach in terms of minimizing forwarder nodes. The number of needed forwarder nodes obtained through EPMR solution is from 40% to 95% of that required by PMR solution in the presence and absence of physical attacks. The performance enhancement is more obvious with small lifetime values. The reason for better performance with small lifetime is because, when the required network lifetime is small, using the EPMR solution it is only necessary to deploy forwarder nodes to maintain the required lifetime. The PMR solution, on the other hand, deploys more nodes in the network initially in order to guarantee a distance between nodes of d_{char}. We also see that n^f increases with an increase in the required lifetime and number of attacks, which naturally follows our expectation. In the rest of this section, we use the EPMR solution to obtain n_f.

Fig. 6 shows the sensitivity of n^f to λ with different lifetimes when the attack size is fixed as 20 m. We make the following observations: First, the required number of forwarder nodes, n^f, is sensitive to the

TABLE II. Simulation Parameters

Parameter	Value
λ	1/500000s to 1/250s
T	1 to 6 days
A	0 to 50 meters
C*	0.6*C(0)
n^s	5000
D	1000 meters
cf	≥ 95%

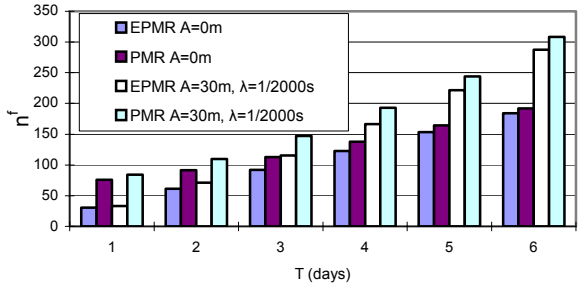

Figure 5. Comparison between EPMR solution and PMR solution.

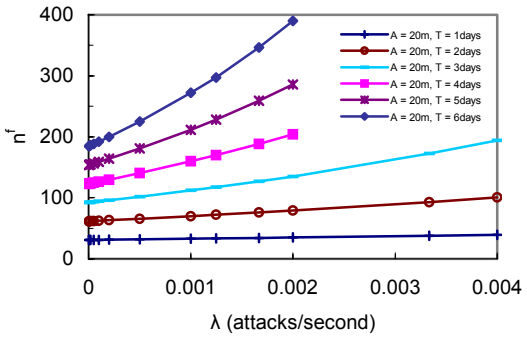

Figure 6. Sensitivity of n^f to λ.

physical attack rate, λ. When λ is big, the attack occurs more frequently. More forwarder nodes are needed in this case to meet the desired network lifetime.

Second, the sensitivity of n^f to λ is more pronounced with larger λ. When λ is very big, the attacks come in very frequently. Here, a little increase in λ can increase the attack intensity significantly. This change greatly increases the required n^f. However, when λ is small, the attacks occur infrequently. In this case, n^f is not too sensitive to λ. This is because when the physical attack comes in very infrequently, fewer nodes are destroyed over a certain period of time. In such cases, n^f is mainly decided by the power consumption of the forwarder nodes. The impact of the physical attacks is not the deciding factor when the attacks are infrequent. In this situation, a change in λ will not prompt drastic changes in n^f.

Third, n^f is sensitive to sensor network lifetime, T. When the network lifetime increases, the sensitivity of n^f to attack interval increases. The reason is that the number of nodes destroyed by the physical attacks increases over time.

Fourth, when λ is too large, long lifetimes cannot be achieved no matter how we deploy the forwarder nodes. In this situation, too many sensor nodes are destroyed by physical attack in a short amount of time and the remaining sensor nodes cannot provide enough throughput to keep the network "alive". As shown in Fig. 6, when λ is larger than 0.002/s, the lifetime, T, of more than 3 days cannot be guaranteed.

Fig. 7 shows the sensitivity of n^f to A, with different lifetime T, and a fixed λ of 1/2000s. The figure shows that n^f increases with increasing attack size, A. The reason is that, the larger the attack size, the bigger the impact of each physical attack. This, in turn, requires more forwarder nodes be deployed initially to maintain the forwarding task.

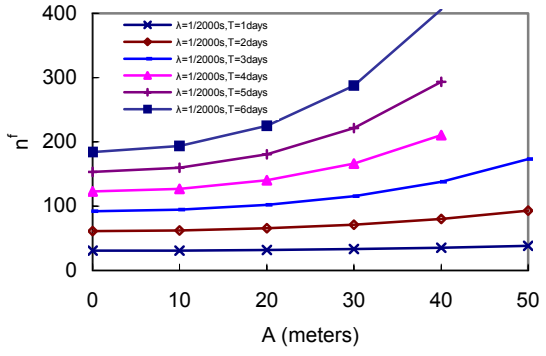

Figure 7. The sensitivity of n^f to A.

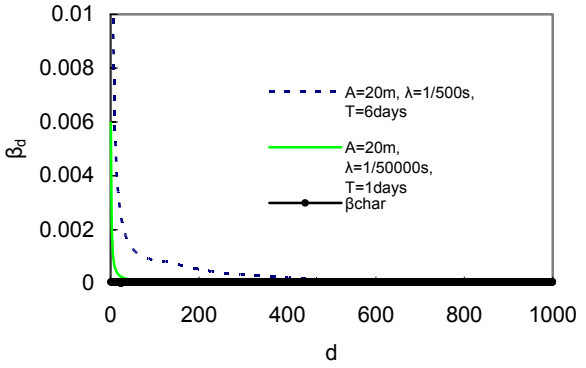

Figure 8(a). The sensitive of β_d to d.

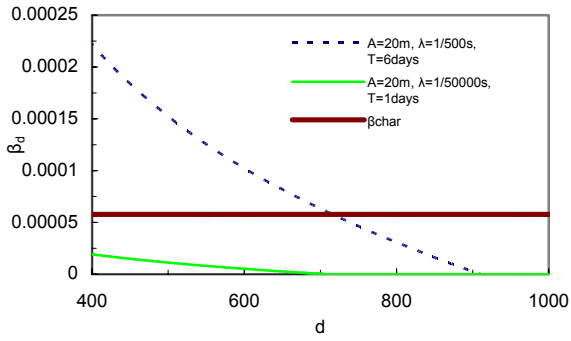

Figure 8(b). The sensitive of β_d to longer values of d.

Fig. 8(a) shows the density of forwarder nodes and the sensitivity of β_d to the distance from the BS under different attack environments and lifetime requirements. The density of required forwarder nodes decreases rapidly with distance, d. This is because there must be a larger number of forwarder nodes near the BS (with small d) to forward the large volume of traffic destined for the BS. Also, the area which these forwarder nodes occupy is very small. When d is large (far away from the BS), the forwarding overhead on each forwarder node is small. Therefore the necessary forwarder node density is small in the areas farther away from the BS. Thus, the density of forwarder nodes decreases as we move from the BS to the perimeter of the network.

In Fig. 8(b), we plot β_d with respect to longer distances (d) away from the BS. We enlarge the right hand part of Fig. 8(a) to plot Fig. 8(b). Across most of the network in an infrequent attack and short lifetime environment the optimal forwarder node deployment has a small node density and does not guarantee a hop distance of d_{char} between nodes sending and forwarding packets. The density is low because this optimal deployment only uses the necessary number of forwarder nodes in order to maintain the required throughput for the required lifetime. The lower curve in Fig. 8(b) is an example of

this fact. On the other hand, when the physical attack is frequent and the required lifetime is long, many forwarder nodes are deployed. This guarantees d_{char} for most areas in the network and is depicted by the upper curve in Fig. 8(b). We summarize our observations in this section as follows:

(1) The optimal n^f is the minimum number of forwarder nodes that can guarantee that forwarder nodes do not run out of power before the desired network lifetime is reached. This does not necessarily depend on the d_{char} assumption. Our solution shows a significant improvement over the *PMR* method in terms of number of deployed forwarder nodes.

(2) The node density at different areas in the network is based on the power consumed by forwarding sensor node traffic. The forwarder nodes in the area near the BS need to forward more traffic. Thus, the area nearest to the BS has the highest density of forwarder nodes, and the density decreases from this area towards the boundary of the sensor network.

(3) The attack parameters and required lifetime impact the node density and n^f. In general for larger A, λ, and T, the node density and n^f are larger.

VI. Final Remarks

In this paper we address an important lifetime problem where a 2- tier sensor network should sustain a minimum throughput for a specified lifetime in environments where physical attacks are present. The problem is in determining optimal deployment of forwarder nodes (top tier) nodes in the network to meet the lifetime requirement.

We first provide a derivation for throughput in our sensor network and derive an expression for the deployment strategy to satisfy the lifetime. We proposed 2 solutions to address this problem. The Power-Minimization Routing based, *PMR*, solution deploys nodes only attempting to minimize energy consumption during routing. We showed that this approach may not always be optimal. We then proposed the Enhanced Power-Minimization Routing based, *EPMR*, solution that deploys nodes *optimally* taking into account, both energy minimization and lifetime requirement.

We make the following important observations: First, the lifetime and number of forwarder nodes required is indeed sensitive to physical attacks. Second, the optimal forwarder node density decreases progressively away from the BS towards the boundary of the sensor network. Third, the optimal forwarder node density does not need to guarantee that each hop distance is the characteristic distance, d_{char} defined in [1]. Fourth, to minimize the number of forwarder nodes, forwarder nodes are deployed only in selected regions of the sensor network.

Lifetime is an important problem in sensor networks. While there has been previous work on sensor network lifetime, we believe that our work is the first to address this issue in the presence of physical attacks. We have made several important observations highlighted above in this realm. The physical attack model we define is highly representative of threats in a sensor network and, to be best of our knowledge has not been addressed in any previous works. As such, we believe that our attack model, or suitable versions of it can be used to test overall sensor network performance/ resilience especially when operating under hostile environments.

References

[1] M. Bhardwaj, A. Chandrakasan, and T. Garnett, " Upper bounds on the lifetime of sensor networks," *Proc. IEEE ICC '01,* pp. 785-790, 2001.

[2] M. Bhardwaj and A. Chandrakasan, "Bounding the lifetime of sensor networks via optimal role assignment," *Proc. IEEE Infocom '02,* pp. 1587-1596, 2002.

[3] Z. Hu and B. Li, "On the fundamental capacity and lifetime of energy-constrained wireless sensor networks," *Proc. IEEE RTAS '04*, pp. 38-47, 2004.

[4] Z. Hu and B. Li, "Fundamental performance limits of wireless sensor networks," to appear in *Ad Hoc and Sensor Networks,* Yang Xian and Yi Pan, Editors, Nova Science Publishers, 2004.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," *International Conference on System Sciences*, January 2000.

[6] M. Kochal, L. Schwiebert, and S. Gupta, "Role-based Hierarchical Self Organization for Wireless Ad hoc Sensor Networks," *Proc. ACM WSNA '03*, pp. 98-107, 2003.

[7] K. Chakrabarty, S. Iyengar, H. Qi, and E. Cho, "Grid coverage for surveillance and target location in distributed sensor networks," *IEEE Transactions on Computers,* vol. 51, No. 12, pp. 1448-1453, December 2002.

[8] T. Clouqueur, V. Phipatanasuphorn, P. Ramanathan, and K. Saluja, "Sensor deployment strategy for target detection," *Proc. ACM WSNA '02*, pp. 42-48, September 2002.

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeaures," *IEEE International Workshop on Sensor Networks*, May 2003.

[10] A. Wood and J. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, pp. 54-62, 2002.

[11] J. Reason and J Rabaey, "A study of energy consumption and reliability in a multi-hop sensor network," *ACM SIGMOBILE Mobile Computing and Communications Review,* vol. 8, num. 1, pp. 84-97, January 2004.