Lifetime Optimization of Sensor Networks under Physical Attacks

Xun Wang, Wenjun Gu, Sriram Chellappan, Kurt Schosek, Dong Xuan
{wangxu, gu, chellapp, schosek, xuan}@cse.ohio-state.edu
1-614-292-2958

Department of Computer Science and Engineering,
The Ohio State University, Columbus, OH 43210

***Abstract*—In this paper, we address a *Resource Constrained Lifetime Problem* in sensor networks in an operating environment subject to physical node destructions. Specifically, given a limited number of sensors, our goal is to maximize the network lifetime and derive the deployment plan of the nodes to maximize the lifetime under physical node destructions. The problem of physical destructions due to hostile environmnets and small size of the sensors is a potent threat and severely constrains the practical lifetime of sensor networks. The lifetime problem we define is representative, practical and encompasses other versions of similar problems. We also define a representative physical attack model under which we study and solve the lifetime problem. Our solutions take into account both the energy minimization and node constraints. We make several observations in this realm of which an important one is the high sensitivity of lifetime to physical attacks highlighting the importance of our study. Our work has broad and immediate impacts to system designers during network deployments in hostile environments.**

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

Lifetime Optimization of Sensor Networks under Physical Attacks

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

***Abstract*—In this paper, we address a *Resource Constrained Lifetime Problem* in sensor networks in an operating environment subject to physical node destructions. Specifically, given a limited number of sensors, our goal is to maximize the network lifetime and derive the deployment plan of the nodes to maximize the lifetime under physical node destructions. The problem of physical destructions due to hostile environmnets and small size of the sensors is a potent threat and severely constrains the practical lifetime of sensor networks. The lifetime problem we define is representative, practical and encompasses other versions of similar problems. We also define a representative physical attack model under which we study and solve the lifetime problem. Our solutions take into account both the energy minimization and node constraints. We make several observations in this realm of which an important one is the high sensitivity of lifetime to physical attacks highlighting the importance of our study. Our work has broad and immediate impacts to system designers during network deployments in hostile environments.**

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

I. INTRODUCTION

Advances in wireless sensor technologies have increased the pace towards realization of a wide variety of sensor network applications dramatically. The key shortcoming in the practical deployment of sensor networks however, is their low energy availabilities that constrain their lifetimes. Sensors can quickly run out of power. This problem is worsened when sensors have to operate in inaccessible environments. In such situations, recharging or replacing the sensors if they die out of power is not practical. Increasing the operational lifetime of sensor networks given their limited energy resources has been and still is a major focus of research in the community [1,2,3,4].

Advances in the miniaturization technologies have significantly shrunk the size and form factor of sensors today. Operation in hostile and uncontrolled environments and the small size of these sensors introduces the additional problem of physical vulnerabilities of the sensor nodes. Such hostile environments are subject to vulnerabilities due to tremors, landslides, falling trees etc. that can result in physical destructions of geographically contiguous sensor nodes. This damage will reduce the overall lifetime of the sensor network. Thus, results on lifetime that have been derived before [1, 2, 3, 4], although theoretically exciting are reduced dramatically when the network operates in physically hostile environments. While the lifetime problem is nevertheless very important, its practical applicability in the realm of sensor networks is closely intertwined with operating conditions, an important facet of which is physical vulnerabilities of the sensor nodes.

The operational lifetime and the effectiveness of the sensed data are the critical factors in the deployment of sensor networks. Our definition of lifetime in this paper is the period of time a sensor network can maintain a certain minimum throughput. Obviously, throughput is a measure of the effectiveness of the sensed data. In this paper, the sensor network model we consider is a 2-tier hierarchical model. Here 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, we address a *Resource Constrained Lifetime Problem* as follows. Given a certain number of forwarding nodes, calculate the maximum lifetime and determine how the nodes must be deployed in order to achieve maximum lifetime when the network is subjected to physical attacks. Our approach to address the deployment problem takes into account both energy minimization and node constraints.

The lifetime problem we address in this paper is significant. Maximizing 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 discuss the system and attack models formally. Section III discusses the problem statement and the solution in detail. We present the performance evaluation in Section IV. Section V discusses related work, and we conclude our study in Section VI.

Manuscript received September 1, 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.

II. System and atttack Models

In the following, we define our sensor network, attack model and terminologies used in the rest of the paper.

A. Sensor Network Model

The sensor network environment (or sensor field) we study is 2-tier and consists of n^s uniformly randomly deployed sensor nodes and n^f forwarder nodes. Sensor and Forwarder nodes each have e^s, e^f joules of initial energy respectively. The sensor nodes continuously transmit data at a rate r intended for the base station (BS) similar to the models used in [3,4,12]. The power loss model we assume in this paper is similar to that in

TABLE I. Notations, Definitions and Standard Values

Notation	Definition	Value
α_1	Receiver energy factor	180nJ/bit
α_2	Transmitter energy factor	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 data rate of each sensor	2kbps
d_{char}	Characteristic distance	134.16 meters
T	Desired lifetime	
$C(t)$	Throughput at time t	$C(0) = n^s * r$
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	
$B(d)$	Density of forwarder nodes at distance d from BS	
D	Sensor network radius	
cf	Confidence interval	

[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

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

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, instead their task is to forward the traffic generated by the sensor nodes in the whole network area to the BS. The data is relayed using one or more 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).

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

$$\Pr[N = k, t] = \frac{e^{\lambda \cdot t} \cdot (\lambda \cdot t)^k}{k!}. \quad (2)$$

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.

III. Resource constrained lifetime optimzation under physical attacks

A. Problem Setup

In the following, we define a scenario where, the sensor network is a circular region of radius, D. The BS is located in the center of the field. Attack events occur following a Poisson distribution with rate λ and are geographically uniformly distributed. Attack events destroy a circular region of radius, A. Sensor nodes continuously transmit data to the BS using forwarder nodes as relays. The deployment of forwarder nodes should ensure that the entire sensor network is covered. The effectiveness of the sensor network is measured by the lifetime until which a desired overall throughput is 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, given a number of forwarder nodes, n^f, given the initial energy of each sensor node, e^s and that of forwarder node, e^f, and given the data rate from each sensor node, r, 1) what is the maximum lifetime that can be attained by the network and 2) how to geographically deploy the forwarder nodes in the network to

[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].

forward all alive sensor nodes' data to the BS while still maintaining a minimum throughput C^* with a confidence, *cf*, in the presence of physical attacks.

While in this paper the sensor field is circular, our work can be easily extended when this is not the case. We discuss the corresponding extension later. The problem we address in this paper is significant. Designers typically are faced with the problem of maximizing the usage of the resources available at their disposal. Using our approach here, sensor network designers will be able to maximize the network lifetime through optimal network deployment of limited node resource. In fact, the problems due to hostile operating conditions of the sensor further enrich the potential importance of our work considering the already limited lifetime of the sensors.

B. Our Solution

We solve a resource constrained lifetime and a deployment problem in this paper. The output of our solution is not just the maximum lifetime but also a detailed deployment plan for the forwarder nodes. The deployment plan will show how many forwarder nodes to deploy where. We use the density of forwarder nodes at distance d away from the BS (denoted as $\beta(d)$) to quantify the deployment. The following are the main challenges in this regard. We have to deploy the available number of forwarding nodes efficiently. The efficiency here relates to overall lifetime, throughput, coverage and power aware routing in the presence of physical attacks. Due to convergence, the forwarder nodes towards the BS receive more traffic than those progressively away from the BS. Thus more nodes nearer to the BS are necessary. Different forwarder node density at different area implies the different distance for a hop in different area during relaying packets to BS. However the presence of physical attacks could destroy a contiguous portion of nodes introducing several challenges: throughput and traffic overhead on forwarder nodes keep changing under attack; the node density and corresponding hop distance traveled in each hop is also impacted by the attack.

1). *The Pseudo-code of our solution*

We provide a pseudocode of our solution to the lifetime and deployment problem in Figure 1. The output of the pseudocode is the maximum lifetime T_{max} and the optimal deployment plan of the forwarder nodes to attain the lifetime. Our solution for the deployment strategy quantifies the number of forwarder nodes to be deployed progressively away from the BS. This obviously is sensitive to the distance from the BS. We denote the optimal density of forwarder nodes at a distance d away from the BS as $\beta^{opt}(d)$. With available resources in terms of forwarding nodes, obviously, the lifetime is impacted by power consumption of the total network, which again is impacted by the routing efficiency.

The first step of our solution is to calculate the upper bound lifetime T_{ub} assuming enough forwarder nodes, optimum routing and minimum power dissipation. We then converge to the attainable maximum lifetime T_{max} due to the constraints using binary search.

Referring to Figure 1, we can see that the pseudocode contains two loops. The outer ***do*** loop computes the lifetime T_{max} using binary search. The outer loop uses the inner ***for*** loop to determine optimal deployment $\beta^{opt}_{est}(d)$ given the estimated lifetime T_{est}. The total number of forwarder nodes needed n^f_{est} for T_{est} is compared with the available number of forwarder nodes n^f. Recursively, we converge to T_{max} when n^f_{est} matches n^f. The outer ***do*** loop starts from T_{ub} to do binary search, aiming to get the optimal T_{max}. We will discuss the derivation of T_{ub} later.

The input for the inner ***for*** loop is the T_{est}. The deployment $\beta(d)$ should sustain this T_{est}. There are two orthogonal dimensions that impact $\beta(d)$ in this regard. The first is the density that can guarantee the minimum energy in the routing [1]. Such a deployment denoted as β_{char} must guarantee a hop distance of d_{char} derived from [1]. d_{char} is given by $d_{char} = \sqrt[n]{\alpha_1/(\alpha_2 \cdot (n-1))}$. β_{char} is obtained from d_{char} by the mapping function, say G(.) between $\beta(d)$ and the routing distance, denoted as d', of nodes at a distance d away from the BS. Such function reflects the geographic relationship between $\beta(d)$ and d'. In this study, we adopt a simple but reasonable function: $\beta(d) = G(d') = 1/d'^2$. With this mapping function, $\beta_{char} = 1/d^2_{char}$ Since in the inner loop we want to minimize the number of forwarder nodes instead of total energy consumption, forwarder node deployment following β_{char} may not necessarily achieve minimum number of forwarder nodes.

We denote $\beta_{low}(d)$ *as* the minimum forwarder node deployment computed by power consumption under the assumption that the routing distance is d_{char}. The way to get $\beta_{low}(d)$ will be explained later. It is simple to see that when $\beta_{low}(d) \geq \beta_{char}$, the power requirements can be met, while the assumption on the routing distance can be held. Thus in this case, $\beta_{low}(d)$ is the optimal deployment under T_{est}, which is $\beta^{opt}_{est}(d)$. However when $\beta_{low}(d) < \beta_{char}$, the assumption on the routing distance when calculating $\beta_{low}(d)$ can not be held anymore. Hence the energy consumption is not optimal and real energy consumption is larger. That means we need to deploy more forwarder nodes than $\beta_{low}(d)$ to satisfy the power consumption rate. Actually the optimal deployment under T_{est}, $\beta^{opt}_{est}(d)$, in this case falls between $\beta_{low}(d)$ and β_{char}.

In the case when $\beta_{low}(d) < \beta_{char}$, we will employ a binary search approach to calculate $\beta^{opt}_{est}(d)$ under the estimate lifetime T_{est} at the inner ***for*** loop. We first use an estimated forwarder node density $\beta_{est}(d)$ to calculate the corresponding estimated routing distance $d_{est}(d)$ by $d_{est}(d) = \sqrt{1/\beta_{est}(d)}$, then we use T_{est} and $d_{est}(d)$ to calculate the node deployment $\beta_{low}(d)$. If $\beta_{low}(d)$ doesn't match $\beta_{est}(d)$, we replace $\beta_{est}(d)$ by $\beta_{low}(d)$ to compute a new $\beta_{low}(d)$. Recursively thus, we converge to $\beta^{opt}_{est}(d)$ when $\beta^{opt}_{est}(d) = \beta_{low}(d) = \beta_{est}(d)$. The integration of $\beta^{opt}_{est}(d)$ is the total number of needed forwarder nodes, n^f_{est} for T_{est}.

Input:
System Side: n^s, n^f, D, r, C^*, cf, e^s, e^f, α_1, α_2, n
Attack side: λ, A

```
While (1) {
Use C*, λ and cf to get T_ub
Choose T_est = T_ub
T_left = 0, T_right = T_ub
do {
    for d = 0 to D {
        Use α_1, α_2 and n to get d_char
        Use d_char to get β_char
        Use d_char as d_est(d) to get β_low(d)
        If β_char ≤ β_low(d)
            β^opt_est(d) = β_low(d)
        else
            Use binary search to get β^opt_est(d) in [β_low(d), β_char]
    }
Summarize β^opt_est(d) to get n^f_est
if n^f_est > n^f
    T_right = T_est
    T_est = (T_left + T_right)/2
else
    T_left = T_est
    T_est = (T_left + T_right)/2
}until (n^f_est = n^f)
T_max = T_est
β^opt(d) = β^opt_est(d)
break;
}
```

Output:
T_{max}, $\beta^{opt}(d)$

Figure 1. Pseudocode

In the following, we discuss how to calculate T_{ub} and $\beta_{low}(d)$.

2). *Derivation of lifetime upper bound - T_{ub}*

Recall that our problem is maximizing lifetime of the sensor network for a given number of forwarder nodes in the presence of physical attacks. For the pseudocode given in Figure 1, we need the upper bound of the lifetime T_{ub} to do the binary search. We can obtain this value based on the requirement of the throughput in the network in the presence of physical attacks.

Intuitively, the throughput in the network in our case is the product of the total number of alive nodes times the sending rate, r. Thus the throughput at time t is given by

$$C(t) = \pi \cdot D^2 \cdot \alpha \cdot \left((D^2 - A^2)/D^2\right)^{m(t)} \cdot r. \qquad (3)$$

In (3), $\left((D^2 - A^2)/D^2\right)^{m(t)}$ denotes the percentage of nodes remaining alive after $m(t)$ attack events (after time t) assuming an attack area of A and a sensor network radius D. The maximum number of attacks M until which the minimum throughput requirement of C^* can be sustained is derived from the following equality

$$\pi \cdot D^2 \cdot \alpha \cdot \left((D^2 - A^2)/D^2\right)^{M} \cdot r = C^*. \qquad (4)$$

Once M is obtained, we can get T_{ub} under our assumed attack model. Recall that we assume a Poisson arrival for the attacks, with a confidence interval cf, T_{ub} is given by the maximum value of t, such that the following inequality is satisfied.

$$\sum_{i=0}^{M} \Pr(N = i, t) \geq cf \ . \qquad (5)$$

In (5), $\Pr(N = i, t)$ is given by equation 2, the probability that i attacks happen in the network during time interval t.

3). *Computing the node deployment- $\beta_{low}(d)$*

This section explains the details of deriving $\beta_{low}(d)$ given the estimated lifetime T_{est} and the estimated routing distance for the forwarder nodes at a distance d away from the BS $d_{est}(d)$.

We denote the power consumption rate of a forwarder node at a distance d from the BS at time t as $p_d^f(t)$. $p_d^f(t)$ is impacted by the forwarder node density $\beta(d)$, since the power consumed by a forward node at a distance d away from the BS at time t depends on the forwarder node density at a distance d away from the BS at time t. Hence, $p_d^f(t)$ is a function of $\beta(d)$. Note however that $p_d^f(t)$ is constrained by the initial energy available at the forwarder node e^f, given below,

$$\int_{t=0}^{T_{est}} p_d^f(t) \cdot dt \leq e^f \ . \qquad (6)$$

Since $p_d^f(t)$ is a function of $\beta(d)$, we thus get an inequality in $\beta(d)$ from (6). We can solve this inequality to obtain the minimum $\beta(d)$, which is $\beta_{low}(d)$. We now discuss the derivation of $p_d^f(t)$.

In order to derive $p_d^f(t)$, we need to get the formulas for the following; $l_d^f(t)$, the total amount of traffic rate in bits/s from the sensor nodes whose traffic needs to be forwarded by the forwarder nodes at distance d away from BS at time t; $n_d^f(t)$, the total number of forwarder nodes at distance d away from BS at time t; and $\overline{p}_d^f(t)$, the average power consumption to relay one bit of data for a forwarder node that is at a distance d away from the BS at time t. Under optimal deployment, the traffic load is uniformly distributed among all forwarder nodes at the same distance away from BS. Hence, the traffic load in bits for each forwarder node at distance d away from BS at time t is $l_d^f(t)/n_d^f(t)$ and $(l_d^f(t)/n_d^f(t)) \cdot \overline{p}_d^f(t)$ means the power consumption rate for each forwarder node at distance d away from BS at time t, which is $p_d^f(t)$.

We introduce the concept of region here to compute the three variables mentioned above. Consider a circle (C_A) of radius $d + d'/2$ and another circle (C_B) of radius $d - d'/2$ (where d is the distance from the BS). We define a region as the area covered by circle C_A and not covered by circle C_B. Its width is d', and is given by $d' = d_{est}(d) = \sqrt{1/\beta_{est}(d)}$, in which $\beta_{est}(d)$ is the estimated forwarder node density at distance d away from BS and $d_{est}(d)$ is the estimated routing

distance of the forwarder nodes that are at a distance d away from the BS. Here we first discuss the case where the forwarder node is at least d' away from the BS. We will discuss the case where the distance of the forwarder node from the BS is less than d' later.

In the case where the forwarder node is at least d' away from the BS, the forwarder node needs to find another forwarder node to forward the traffic. Since the width of this region is d', the routing distance of the forwarder nodes that are at a distance d away from the BS, the traffic in this region will be forwarded by the forwarder nodes in this region once and only once. So we can derive the formulas for $l_d^f(t)$, $n_d^f(t)$ and $\bar{p}_d^f(t)$ as given below.

$$l_d^f(t) = \int_{u=d+d'/2}^{D} 2\cdot\pi\cdot u\cdot du\cdot\alpha\cdot\left((D^2-A^2)/D^2\right)^M\cdot r. \quad (7)$$

$$n_d^f(t) = \int_{u=d-d'/2}^{u=d+d'/2} 2\cdot\pi\cdot u\cdot\beta(u)\cdot\left((D^2-A^2)/D^2\right)^M du. \quad (8)$$

$$\bar{p}_d^f(t) = \int_{u=d'/2}^{3\cdot d'/2}(\alpha_1+\alpha_2 u^n)\cdot \Pr(u)\cdot du. \quad (9)$$

Here *Pr(u)* means the distribution function of routing distance of the forwarder nodes that are at a distance u away from the BS. We will explain the derivation of *Pr(u)* below.

For the forwarder nodes whose distance from the BS, *d,* is less than d', their next transmission distance is always *d* since the BS is in their one hop transmission range. 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'. 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

$$\Pr(u) = \begin{cases} 1/d', & where\ d > d' \\ 1, & where\ d \le d', u = d \\ 0, & where\ d \le d', u \ne d. \end{cases} \quad (10)$$

The case we study above considers when the distance of the forwarder node from the BS is at least d'. It is easy to extend the above formula to the case that $d< d'$ by just replacing d' with *d*. Combining equations (7), (8), (9) and (10) using the relationship $p_d^f(t) = (l_d^f(t)/n_d^f(t))\cdot\bar{p}_d^f(t)$, we get $p_d^f(t)$ given below.

$$p_d^f(t) = \begin{cases} \dfrac{[D^2-(d+d'/2)^2]\cdot\alpha\cdot r}{2\cdot d\cdot d'\cdot\beta(d)} \cdot\int_{u=d'/2}^{3\cdot d'/2}(\alpha_1+\alpha_2 u^n)\cdot\dfrac{1}{d'}\cdot du, \\ \qquad where\ d \ge d'\ \ and \\ \dfrac{[D^2-(3\cdot d'/2)^2]\cdot\alpha\cdot r}{2\cdot d^2\cdot\beta(d)}\cdot(\alpha_1+\alpha_2 d^n), \\ \qquad where\ d < d'. \end{cases} \quad (11)$$

From (11) the minimum $\beta(d)$ is calculated such that the constraint in (6) is satisfied, which is $\beta_{low}(d)$.

IV. Performance Evaluation

In this section, we report the numerical result based on the analysis in Section III. Our first motivation is to show the maximal lifetime with different forwarder nodes number, nf. We also wish to study the impacts of physical attacks on the sensor network lifetime. 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 rate λ. Each event destroys a circular region of radius A. The attacks are uniformly geographically distributed. Table I in Section II 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).

TABLE II. SIMULATION PARAMETERS

Parameter	Value	Parameter	Value
λ	1/500000s to 1/250s	C^*	0.6*$C(0)$
		n^s	5000
n^f	50 to 600	D	1000 meters
A	0 to 50 meters	cf	95%

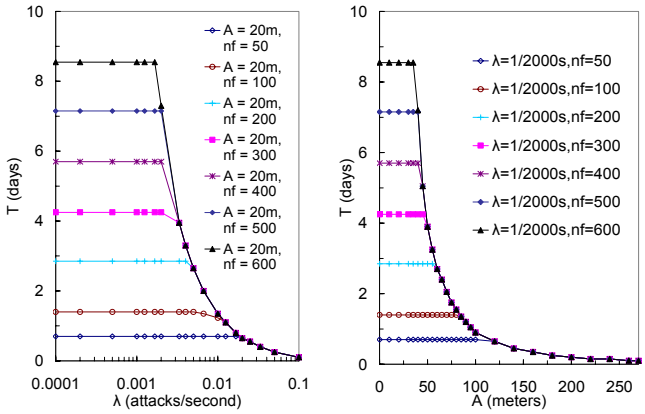
We use MATLAB to get the performance data based on the formulas derived in Section III. Note that T in this section refers to the maximum lifetime (T_{max} in section III) and $\beta(d)$ refers to $\beta^{opt}(d)$ in Section III.

Fig. 2(a) shows the sensitivity of T to λ with different forwarder nodes number, n^f, when the attack radius A is fixed as 20 m. We make the following observations: First, the network lifetime, T, is sensitive to the number of available forwarder nodes, n^f. More available forwarder nodes, the traffic overhead on each forwarder node is small, and the power consumption rate of each forwarder node is small resulting in longer lifetimes of each forwarder node. Hence, the network can maintain the required throughput longer and network lifetime, T, is prolonged.

Second, T is sensitive to the physical attack rate, λ. When λ is big, the attacks occur more frequently. The loss of throughput makes the network lifetime smaller.

Third and most importantly, T is only decided by n^f when λ is small, and is only decided by λ when λ is big enough for given n^f. When λ is small, the attacks decrease the throughput slowly, under which situation, the forwarder nodes will be out of power before the throughput goes below C^*. With our optimal forwarder node deployment, the forwarder node's power consumption rate will not be changed under attack (because the density of forwarder nodes and sensor nodes decrease with same rate under attack). Only n^f decides the forwarder node's power consumption rate, which decides the lifetime of the network if forwarder nodes exhaust the power before the throughput decreases below C^* by the attacks. This corresponds to the case when $T_{max}<T_{ub}$ in Section III. However, when λ is big, the throughput of the network will decrease below C^* due to attacks, before forwarder nodes are out of power. For certain n^f, there is a threshold value of λ, referred as $\lambda(n^f)$. When $\lambda<\lambda(n^f)$, T is decided by n^f, which

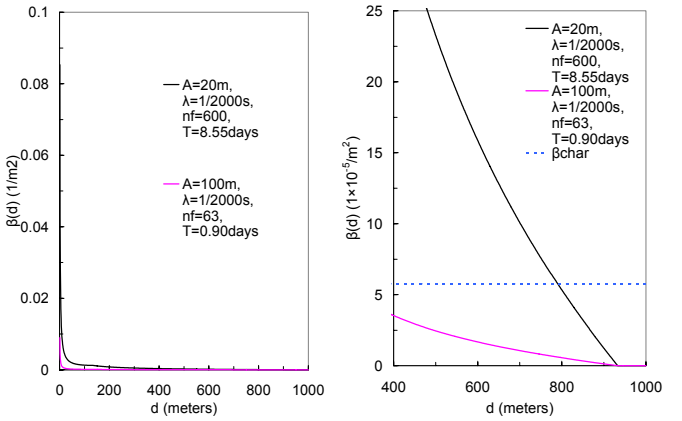
decides the power consumption rate and lifetime of each forwarder node; when λ is big enough, i.e. $\lambda > \lambda(n^f)$, T is decided by λ and this corresponds to the case $T_{max} = T_{ub}$ in Section III.



(a) The sensitivity of T to λ. (b) The sensitivity of T to A.

Figure 2. The sensitivity of T to λ and A.

Fig. 2(b) shows the sensitivity of T to A, with different forwarder nodes number, n^f, and a fixed λ of 1/2000s. The figure shows that T decreases with increasing attack size, A. The reason is that; larger the attack size is, bigger is the impact of each physical attack. Similar to the observation we made earlier, when A is smaller than certain value (decided for given n^f), T is only decided by n^f and $T_{max} < T_{ub}$; otherwise, T is decided by A and $T_{max} = T_{ub}$.



(a) The sensitive of $\beta(d)$ to d. (b) The sensitive of $\beta(d)$ to large d.

Figure 3. The optimal forwarder node deployment $\beta(d)$.

Fig. 3(a) shows the density of forwarder nodes and the sensitivity of $\beta(d)$ to the distance, d, from the BS under different attack environments and with different n^f. The density of required forwarder nodes decreases rapidly with distance, d. This is because there must be a large number of forwarder nodes in the small area near the BS (with small d) to forward the large volume of traffic destined for the BS, resulting in a high density, $\beta(d)$, in this area. 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.

(1) In Fig. 3(b), we plot $\beta(d)$ with respect to longer distances (d) away from the BS. We enlarge the right hand part of Fig. 3(a) to plot Fig. 3(b). In the situations where n^f is small or d is big, 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 minimal node density guaranteeing d_{char} is shown as β_{char} in this figure. When d is big, the density is low because our optimal deployment only uses the necessary number of forwarder nodes in order to maintain the required throughput or because there is not enough forwarder nodes. The curve, in the case where $A=20m$, in Fig. 3(b) is an example where T is only decided by n^f because the attack is not intensive, and $T_{max} < T_{ub}$. The curve, in the case where $A=100m$ is an example where T is dominated by intensive attacks. In this figure, 63 forwarder nodes are enough to achieve the T_{max}. More forwarder nodes will not help because the attack will make the throughput lower than C^* after 0.9 days.

V. Related Work

In wireless sensor networks there have been a few works on the bounds of lifetime and throughput. In [1], Bhardwaj et al. set forth the upper bound of sensor 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}). Using these minimum energy relays they derive the upper bound for a variety of network scenarios. In [2], Bhardwaj et al extend their previous work in [2] 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.

In [3], Hu and Li also focus on the effects that energy constraints have on the lifetime of wireless sensor networks. 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. In [14], Zhang and Hou derive the necessary and sufficient conditions of the node density to maintain k-coverage in the sensor networks, based on which they give the upper bound of lifetime for 1-coverage networks.

In [12], Pan et al. propose algorithms to location the BS to prolong lifetime. 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. On the other hand, Clouqueur et al. propose an algorithm in [8] to determine a deployment strategy in order to detect moving targets, given that only the number and density of nodes in an area can be determined a priori.

While our work has similarities with the previous works, we study how to achieve the maximal lifetime by effective node deployment in a sensor network under the presence of physical attacks. Randomness due to the nature of such attacks makes our problem even more difficult.

Many sensor networks will be deployed in hostile environments. It is in fact an issue of sensor network security, especially if physical destruction of sensor nodes 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. However operations in the presence of physical attacks are not addressed by the above, which is the feature of our work here.

VI. Final Remarks

In this paper we address a *Resource Constrained Lifetime Problem* in a sensor network operating under the threats of physical node destructions. Specifically, we defined a representative lifetime problem and solved it to obtain the maximum lifetime and the detailed deployment plan of the nodes in the presence of physical attacks.

We made important observations. Physical attacks do pose a potent threat to sensor deployment and our data further strengthened this claim. We argued the impact of convergence of the traffic progressively towards the BS that resulted in a location aware variable deployment density for the forwarder nodes. We also pointed out the difference between optimal energy routing and lifetime maximization and showed why guaranteeing optimal routing does not necessarily maximize lifetime. When attack is not intensive, the maximum lifetime is decided by the number of forwarder nodes. Under intensive attacks however, the maximum lifetime is decided by attack parameters, in which case, a certain number of forwarders are enough to achieve maximum lifetime. More than this number will not prolong the lifetime.

The sensor network field we study in this paper is circular. However our work can be easily extended to a network of any arbitrary shape. For an arbitrary shaped network field, we can use polar coordinates to quantify the area. With the BS as the Pole, the distance from any point on the boundary of the area can be measured as $r(\theta)$, where r is the distance from the BS and θ is the polar angle for that point. We separate the area into multiple sectors with different radii (depending on $r(\theta)$ at θ) and then apply our proposed method in Section III in each sector to obtain the power consumption rate of forwarder nodes and calculate the deployment in that area. For more details refer to [13].

We believe that our work is the first to study the importance of sensor network lifetime in the presence of physical attacks. Our performance data highlights the sensitivity of performance to physical attacks highlighting importance of our study. 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.

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.

[12] J, Pan, Y. T. Hou, L. Cai, Y. Shi, S. X. Shen, "Topology control for wireless sensor networks," *Proc .ACM MobiCom'034*, pp. 286 – 299, September 2003.

[13] X. Wang, W. Gu, S. Chellappan and D. Xuan, "On Lifetime Optimization of Sensor Networks under Physical Attacks", Technical Report, Dept. of Computer Science and Engineering, The Ohio-State University, August. 2004. Available at http://www.cse.ohio-state.edu/~chellapp/lifetime.pdf.

[14] H. Zhang and J. Hou, "On Deriving the Upper Bound of α-Lifetime for Large Sensor Networks", *Proc .ACM Mobihoc'04*, pp. 121 - 132, 2003.