Sensor Network Configuration under Physical Attacks

Xun Wang, Wenjun Gu, Kurt Schosek, Sriram Chellappan, Dong Xuan

The Department of Computer Science and Engineering
The Ohio State University
Columbus, Ohio 43210, USA
{wangxu, gu, schosek, chellapp, xuan}@cse.ohio-state.edu

Abstract. Sensor networks typically operate in hostile outdoor environments. In such environments, sensor networks are highly susceptible to physical attacks that can result in physical node destructions. In this paper, we study the impacts of physical attacks on sensor network configuration. Lifetime is an important metric during configuration for many sensor applications. While lifetime is constrained by limited energies and has been addressed before, prior results cannot be directly applied in the presence of physical attacks. In this paper, we define a practical lifetime problem in sensor networks under a representative physical attack model that we define. We develop an anlytical approach to derive the minimum number and deployment plan of sensors to meet lifetime requirement under physical attacks. We make several observations in this paper. One of our important observations is the high sensitivity of lifetime to physical attacks highlighting the significance of our study.

1 Introduction

Sensor networks are typically expected to operate in hostile and inaccessible environments. Instances are battlefields, seismic/volcanic areas, forests etc. Attackers can "physically destroy" sensor nodes due to small sizes of the sensors and the distributed nature of their deployment. We term such attacks as *Physical attacks*. Physical attacks are patent and potent in sensor networks. Attacks can range from a simple and low cost brute force destruction of sensor nodes like bombs, missiles, grenades, moving tanks/vehicles etc. to more intelligent attacks. The end result of physical attacks can be *fatal*. The backbone of the sensor network (the sensor nodes themselves) can be destroyed resulting in severe performance degradation. While much attention has been paid to other types of attacks [1, 2] in sensor networks, to the best of our knowledge threats due to physical attacks is still unaddressed. We believe that viability of sensor networks in the future is closely intertwined with their ability to resist physical attacks.

In this paper, we study the impacts of physical attacks on sensor network configuration. Specifically the problem we study here is: Given a desired lifetime for which the sensor network must be operational, determine the minimum number of nodes and how they must be deployed in order to achieve the desired lifetime when the network is subjected to physical attacks. While there are other variations of physical attacks, in this paper we study physical attacks in the form of bombs targeted at a sensor network with the intention of destroying the sensors. The problem is significant and practical. Lifetime is one of the most important metrics during sensor network configuration [3, 4, 5, 6]. This is mainly due to the low energy availabilities in today's sensors that constrain their lifetimes. Sensor networks are typically expected to last for a specific duration to sense desired events and the resources have to be procured and deployed accordingly to meet the lifetime objective [7, 8]. Physical attacks are inevitable in sensor networks, and as such the problem we study is significant. While a body of work has appeared in studying lifetime, their results cannot be directly applied in physically hostile environments primarily due to their not considering the threats of physical attacks.

The output of our solution is the minimum number of nodes needed and the deployment plan, which depend on several factors including the nodes deployment, routing strategies, power availability etc. The presence of physical attack introduces randomness along with the above factors, which make the problem more challenging. We propose an analytical approach to solve this problem. The key idea is to determine and deploy the nodes taking into account both energy minimization and lifetime requirement. We conduct both analysis and simulations to validate our approach. Our data show that results obtained through our analysis matches well with simulation. Our data also show that the lifetime of sensor network is indeed sensitive to physical attacks, which further highlight the significance of our work.

2. System Model and Problem Setup

2.1 Sensor Network Model

We consider a 2-tier hierarchical network model here. The sensor network consists of n^s uniformly deployed sensor nodes. Each sensor node initially has e^s joules of energy. Sensor nodes that sense the data use a set of nodes called *forwarder nodes* as relays to continuously transmit their data to the BS. The forwarder nodes do not generate data. They just relay data using other forwarder nodes 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. Each forwarder node initially has e^f joules of energy.

The effectiveness of the sensor network is measured by the overall throughput in bits per second received by the BS. Our analysis in this paper is not constrained by the shape of the area of deployment. However, for ease of understanding of the corresponding derivations, we assume the sensors are uniformly deployed over a circular area of radius *D*, with the area of the network being $\pi \cdot D^2$. The Base Station (BS) is located at the center of the sensor field. All notations, their definitions and standard values are given in Table 1[1].

[1] Empty fields in Column 3 imply that the corresponding parameters are variables in performance evaluation.

Table 1. Notations, Definitions and Standard Values

Notation	Definition	Value	Notation	Definition	Value
α_1	Receiver constant	180nJ/bit	$C(t)$	Throughput at time t	
α_2	Transmitter constant	10pJ/bit/m^2	$C*$	Desired throughput	
n	Path loss factor	2	λ	Attack arrival rate	
e^s	Initial power of sensor node[2]	2200J	A	The radius of the area destroyed per attack instance	
e^f	Initial power of forwarder node[3]	18400J	n^s	Number of sensor nodes	
r	The sending rate	2kbps	n^f	Number of forwarder nodes	
d_{char}	Characteristic distance	134.16 Meters	β_d	Density of forwarder nodes at distance d from BS	
T	Desired lifetime		D	Sensor network radius	
$C(0)$	Initial throughput	n^s *r	cf	Confidence	

In the radio model [3], 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,

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

Assuming a $1/d^n$ path loss [3], 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 1. Forwarder nodes have more energy and can increase their transmission range at the cost of more energy dissipation according to (1).

2.2 Attack Model

In this paper we study physical attacks in the form of bombs targeted at a sensor network with the intention of destroying the sensors. 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. Each attack event destroys a circular region of radius A. In this paper we assume attack events follow a Poisson distribution in time. The probability of k attacks in a time interval t, with a mean arrival rate λ is given by,

$$\Pr[\mathrm{N = k}] = e^{\lambda \cdot t} \cdot (\lambda \cdot t)^k / k!. \tag{2}$$

The attack events are assumed to be uniformly geographically distributed over the sensor field. While the sensor and the forwarder nodes can be destroyed due to attacks, we assume here that the BS will not be destroyed during attacks.

[2] Initial power for sensor node is based on 500mA-hr, 1.3V battery.

[3] Initial power for forwarder node is based on 1700mA-hr, 3V battery which is similar to the PicoNodes used in [9].

2.3 Problem Setup

The problem we address is: Given a sensor network consisting of n^s uniformly distributed sensor nodes that continuously send data to a BS 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 geographic deployment of these nodes in the sensor field such that the lifetime is guaranteed under physical attacks. More specifically, the inputs to our problem are n^s, *D, C*,T, A, λ*. We solve the problem by calculating the optimal number of forwarder nodes at distance *d* away from the BS under physical attacks. We denote the density of forwarder nodes *d* away from the BS 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.

3. Problem Solution

We now discuss how to determine β_d and deployment plan of the forwarder nodes To solve our problem, we need to derive formulas to compute total traffic throughput to BS and power consumption of each forwarder node as follows.

3.1 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 1.

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. The number of sensor nodes whose traffic can reach the BS without considering physical attacks is:

$$S(t) = \alpha \cdot \int_{u=0}^{d_{\min}} 2 \cdot \pi \cdot u \cdot \prod_{i=1}^{H(u,t)} f^{f}_{u - \sum_{k=1}^{i} d_m(k,u,t)}(t) \cdot du. \qquad (3)$$

In (3), 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; $f^f_u(t)$ is 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*; *H(u,t)* is 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; *m(t)* is the number of physical attacks that are expected to arrive in a time period *t*; $d_m(k,u,t)$ is 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*. Due to space limitation, we do not discuss the detail derivations of *S(t)* and d_{min}, $f^f_u(t)$, *H(u,t), m(t)* and $d_m(k,u,t)$. Interested readers can refer to [10].

Clearly $(\pi \cdot D^2 - \pi \cdot A^2) \big/ (\pi \cdot D^2)$ 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. Hence, the number of sensor nodes whose traffic can reach the BS at time *t* under physical attacks is:

$$S^{*}(t)=\alpha\cdot\int_{u=0}^{d_{\min}}2\cdot\pi\cdot u\cdot\prod_{i=1}^{H(u,t)}f^{f}_{u-\sum_{k=1}^{i}d_{m}(k,u,t)}(t)\cdot du\cdot\left((\pi\cdot D^{2}-\pi\cdot A^{2})/(\pi\cdot D^{2})\right)^{m(t)}. \qquad (4)$$

It is now simple to calculate the overall network throughput. 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,

$$C(t)=\int_{u=0}^{d_{\min}}2\cdot\pi\cdot u\cdot\prod_{i=1}^{H(u,t)}f^{f}_{u-\sum_{k=1}^{i}d_{m}(k,u,t)}(t)\cdot du\cdot\alpha\cdot\left((\pi\cdot D^{2}-\pi\cdot A^{2})/(\pi\cdot D^{2})\right)^{m(t)}\cdot r. \qquad (5)$$

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. Thus 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 forwarder node *d* away from the BS and the next hop distance. The traffic load of a forwarder node at distance *d* and time *t*, denoted by $w_{d}^{f}(t)$, is given by,

$$w_{d}^{f}(t)=\frac{\int_{u=u'}^{d_{\min}}2\cdot\pi\cdot u\cdot f_{u}^{s}(t)\cdot du\cdot\alpha\cdot((D^{2}-A^{2})/D^{2})^{m(t)}\cdot r}{\int_{u=d-d'/2}^{u=d+d'/2}2\cdot\pi\cdot u\cdot\beta_{u}\cdot((D^{2}-A^{2})/D^{2})^{m(t)}\cdot du}, \qquad (6)$$

where β_u is the density of forwarder nodes at distance *u* away from BS.

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, their next transmission distance will be $d_{m}(1,d,t)$ .Thus $p_{d}^{f}(t)$ can be given by the following general formula:

$$p_{d}^{f}(t)=\begin{cases}\dfrac{[d_{\min}^{2}-(d+d_{m}(1,d,t)/2)^{2}]\cdot\alpha\cdot r}{2\cdot d\cdot d_{m}(1,d,t)\cdot\beta_{d}}\cdot(\alpha_{1}+\alpha_{2}\cdot d_{m}(1,d,t)^{n}),\ if\ d\geq d_{m}(1,d,t)\\[3em]\dfrac{[d_{\min}^{2}-(d_{m}(1,d,t))^{2}]\cdot\alpha\cdot r}{2\cdot d^{2}\cdot\beta_{d}}\cdot(\alpha_{1}+\alpha_{2}d^{n}),\ \ if\ \ d<d_{m}(1,d,t).\end{cases} \qquad (7)$$

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,

$$n^{f}=\int_{u=0}^{D}2\cdot\pi\cdot u\cdot\beta_{d}\cdot du \qquad (8)$$

Due to space limitation, we do not give detail derivations of throughput *C(t)*, traffic load of a forwarder node $w_d^f(t)$, and power consumption rate $p_d^f(t)$. Interested readers can refer to [10].

3.2 Our Solution

Having derived the formulas to compute *C(t)* and $p_d^f(t)$, our problem can be expressed as in Figure 1. The intuitive way to solve this problem is to deploy forwarder nodes in such way that the energy spent by the forwarding nodes is minimized with the intention of minimizing the total number forwarding nodes. However, we will see this is not always the case.

Objective: Minimize n^f

Constraints:

$\int_{t=0}^{T} p_d^f(t) \cdot dt \le e^f$ (9), $p_d^f(t)$ is given in (7)

$$C(t) = [\int_{u=0}^{d_{\min}} 2\pi \cdot u \cdot \prod_{i=1}^{H(u,t)} f^f_{u-\sum_{k=1}^{i} d_m(k,u,t)}(t) \cdot du] \cdot \alpha \cdot \left((\pi D^2 - \pi A^2)/(\pi D^2)\right)^{m(t)} \cdot r \ge C^* \quad (10)$$

Figure 1. Restated problem description.

Energy consumption is determined by the routing policy. The routing policy includes the number of intermediate forwarder nodes and the transmission distance. In [3], if each forwarder node's transmission distance is equal to the d_{char} in (11), the energy consumption is minimum. In (11), denoting α_1, α_2, and *n* as the receive, transmit amplifier, and path loss constants, we have,

$$d_{char} = \sqrt[n]{\alpha_1 / (\alpha_2 (n-1))} \ . \quad (11)$$

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}. Our solution gives a *lower bound* of the required forwarder nodes number given desired lifetime. Thus, we need a function to relate $\underline{d}$ with the *lower bound* of forwarder node density. We denote the function mapping the network forwarder node density β and $\underline{d}$ as *G(.)*. A reasonable *G(.)* is $\underline{d} = \sqrt{1/\beta}$ or $\beta = 1/\underline{d}^2$. For detailed explanation, refer to [10]. We denote the *lower bound* of 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* $1/(d_{char}^2 \cdot (\pi \cdot D^2 / (\pi \cdot D^2 - \pi \cdot A^2))^{m(t)})$.

With the above routing arrangement, enough forwarder nodes will be available for routing through the entire lifetime to guarantee d_{char}. Formula (10) can be simplified as follows,

$$C(t) = \pi \cdot d_{\min}^2 \cdot \alpha \cdot \left((D^2 - A^2)/D^2\right)^{m(t)} \cdot r \ge C^* . \quad (12)$$

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 (7), (9) and (12) as following.

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 (12), and then β_d^{power} can be computed from (7) and (9). 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.

If β_d^{power} >= β_{char}, our assumption that d_{char} can be guaranteed holds. Otherwise, the forwarder node density of β_d^{power} does not guarantee d_{char}. But the problem is: do we have to guarantee d_{char}? The answer is no. Consider a simple case where each forwarder node has enough 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.

In the case when $\beta_{char} > \beta_d^{power}$, we do not deploy nodes with the intention of guaranteeing β_{char}. Instead we only need to deploy a 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 larger 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 (7), (9) and (12). Thus we obtain the optimum β_d, lying between β_{char} , which gives an upper bound and β_d^{power} , which gives the lower bound of the network density when $\beta_{char} > \beta_d^{power}$.

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

$$d_m(1,u,t) = \max(d_{ch}(u,t), d_{char}), \tag{13}$$

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 $\beta_u(0) = \beta_u$.

4. Performance Evaluation

In this section, we report our performance data based on the analysis in Section 3. We reiterate that our sensor network is a circular region of radius, D=1000 *meters* and BS is located at the center of the region. Attack events follow a Poisson distribution with a rate λ. Each event destroys a circular region of radius A and attacks are uniformly geographically distributed. Throughout our performance evaluation, the desired throughput C^* is set at 60% of the initial throughput $C(0)$, cf = 95%.

Fig. 2 shows the sensitivity of n^f to λ with different lifetimes when the radius of one attack destruction area (A) is fixed as 20 meters. We make the following observations: First, the required number of forwarder nodes, n^f, is sensitive to the 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.

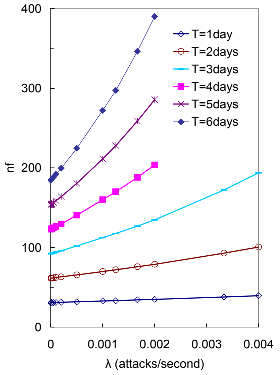


Figure 2. Sensitivity of n^f to λ.

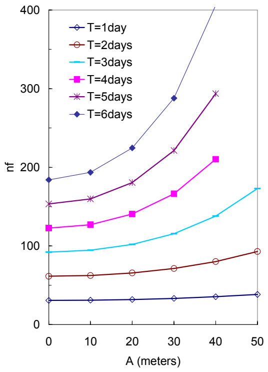


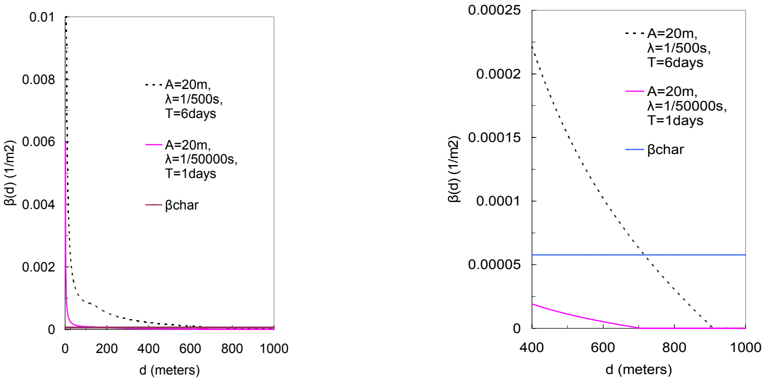
Figure 3. The sensitivity of n^f to A.

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. Third, n^f is sensitive to sensor network lifetime, T. When the network lifetime increases, the sensitivity of n^f to attack rate 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. As shown in Fig. 2, when λ is larger than 0.002/s, the lifetime, T, of more than 3 days cannot be guaranteed.

Fig. 3 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.

Fig. 4(a) shows the density of forwarder nodes and the sensitivity of β_d (deployment) 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.

In Fig. 4(b), we plot β_d with respect to longer distances (*d*) away from the BS. We enlarge the right hand part of Fig. 4(a) to plot Fig. 4(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. 4(b) is an example of this fact. On the other hand, when physical attacks are 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. 4(b).



(a). Sensitivity of β_d to *d*.

(b). Sensitivity of β_d to large *d*.

Figure 4. The optimal forwarder node deployment β_d .

We developed a deployment algorithm for findings of this paper to be practically applied. The basic idea is to separate the entire circular area, whose radius is *D*, into many homocentric rings with small widths. Forwarder nodes based on β_d are randomly, uniformly deployed in each ring. Interested readers can refer to [10] for the details of the algorithm.

6. Final Remarks

Physical attacks are a patent and potent threat in sensor networks. Physical destruction of small size sensors in hostile environments is inevitable. In this paper we studied lifetime of sensor networks under physical attacks. We conducted a detained analysis on how many nodes to deploy and their detailed deployment plan to achieve desired lifetime objectives. Our analysis data matches quite well with simulations, highlighting the fidelity of our analysis. There are several potential directions to extend our study. One of our current focuses is effective counter measuring strategies against physical attacks to enhance the security of the network from physical attacks. We also plan to study impacts due to other forms of physical attacks. Attacks can be intelligent in that they can target nodes to destroy with more sophistication and intelligence raising a host of interesting issues left to be addressed.

References

1. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeaures," *IEEE International Workshop on Sensor Networks*, May 2003.
2. A. Wood and J. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, pp. 54-62, 2002.
3. M. Bhardwaj, A. Chandrakasan, and T. Garnett, "Upper bounds on the lifetime of sensor networks," *Proc. IEEE ICC '01,* pp. 785-790, 2001.
4. M. Bhardwaj and A. Chandrakasan, "Bounding the lifetime of sensor networks via optimal role assignment," *Proc. IEEE Infocom '02,* pp. 1587-1596, 2002.
5. 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.
6. 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.
7. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," International Conference on System Sciences, January 2000.
8. 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.
9. 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.
10. X. Wang, W. Gu, K. Schosek, S. Chellappan and D. Xuan, "Sensor Network Configuration under Physical Attacks", Tech. Report (OSU-CISRC-7/04-TR45), Department of CSE, The Ohio State University, November 2004.