# Policy-driven Physical Attacks in Sensor Networks: Modeling and Measurement

Xun Wang, Sriram Chellappan, Wenjun Gu, Wei Yu, and Dong Xuan

***Abstract*— Sensor nodes being small in size and distributively deployed, are vulnerable to *Physical Attacks* that attempt to physically destroy sensors in the sensor network. Generally speaking, physical attacks in sensor networks can be classified into two types: *Blind Physical Attacks* and *Search-based Physical Attacks*. In blind attacks, sensors are destroyed using brute-force approaches (like bombs/grenades etc.). The advantage here is the rapidness in destroying sensors. The downside however, is the fact that the deployment field also suffers significant casualties. If the attacker wishes to preserve the deployment field, the attacker will conduct search-based attacks by searching for sensors in the field and destroying only the sensors. While this preserves the deployment field, the attack process is slow. In this paper, we present *Policy-driven Physical Attacks*, where the bias between the twin objectives of the attacker (rapidly destroying sensors, and preserving the deployment field) is modeled as a policy for the attacker. In policy-driven physical attacks, the attacker walks through the sensor network deployment field using signal detecting equipment to locate active sensors. Depending on the attacker's policy, the attacker takes different actions during the attack process. Based on detailed performance measurement, we observe that the policy has impacts on the network performance and destruction in the deployment field, demonstrating that the attacker can achieve desired bias in its objectives under policy-driven physical attacks.**

## I. Introduction

The small form factor of sensors, coupled with the unattended and distributed nature of their deployment expose sensor networks to a special class of attacks that could result in the physical destruction of sensors. We denote *Physical Attacks* as those that result in the physical destruction of sensors, thereby rendering them permanently non-operational.

The significance of studying physical attacks comes from the following factors. Physical attacks are *inevitable* threats in sensor networks. Physical attacks are relatively simple to launch and *destructive*. Generally speaking, physical attacks can be classified into two types. In *Blind Physical Attacks* [1], the attacker blindly attacks the sensor network by hurling grenades/bombs in the deployment field and destroys the sensors. In *Search-based Physical Attacks* [2], the attacker detects sensors by moving in the sensor network using signal detection equipment and then destroys only the detected sensors. In any case, the end result of physical attacks can be quite fatal. The backbone of the network (the sensors themselves) is destroyed. Destruction of sensors may also result in the violation of the important network paradigms. A wide spectrum of impacts may result due to physical attacks and when left unaddressed, physical attacks have the potential to render the entire sensor network mission useless.

Xun Wang, Sriram Chellappan, Wenjun Gu and Dong Xuan are with The Department of Computer Science and Engineering, The Ohio State University, Columbus, OH 43210, U.S.A. E-mail: {wangxu, chellapp, gu, xuan}@cse.ohio-state.edu. Wei Yu is with The Department of Computer Science, Texas A & M University, College Station, TX 75082, U.S.A. E-mail: weiyu@cs.tamu.edu.

Both *Blind* and *Search-based Physical Attacks* have their merits and shortcomings. *Blind Physical Attacks*, while destroying many sensors quickly can cause significant casualties to the deployment field. This is an issue, especially when the attacker may want to preserve the deployment field (airports, oil fields, battlefields etc. of the attacker side). On the other hand, in *Search-based Physical Attacks*, the attacker searches for sensors and destroys only the sensors. While this reduces casualties to the deployment field, the attack process is slow in its execution. There are two objectives that are of interest to the attacker when conducting physical attacks. They are; rapidly destroying sensors (i.e., compromising the performance of the sensor network), and minimizing casualties to the deployment field (i.e., preserving the deployment field of the sensor network). In this paper, we define two metrics in this realm. The performance metric that quantifies the attacker's effectiveness in destroying sensors is *Accumulative Coverage (AC)* of the network. $AC$ captures both the lifetime and coverage and as such is an effective metric to measure sensor network performance. The metric that quantifies the attack casualty to the deployment field is *Destruction Casualty (DC)*. $DC$ is the accumulative destroyed area in the sensor network deployment field as a result of physical attacks. Clearly, the above two objectives are conflicting with each other during physical attacks. For rapid destruction, the attacker cannot afford to search for sensors, which means there will be casualties to the deployment field when the network is attacked blindly. Similarly, if the attacker wants to minimize casualties to the deployment field, it has to search for sensors, which means the process cannot be rapid. Typically, depending on its requirements, the attacker will have a degree of *bias* among the two objectives. For instance, if the deployment field is very important, the attacker will prefer search-based attacks, while if rapid destruction of the sensor network is critical, the attacker will prefer blind attacks.

In this paper, we define a new class of physical attacks in sensor networks called *Policy-driven Physical Attacks* in which, the *policy* represents the *bias* among the twin objectives of the attacker. Specifically, the policy is abstracted as a parameter $P$ that quantifies the bias. In our policy-driven physical attack model, the attacker walks through the sensor network deployment field using signal detecting equipment to locate active sensors. However, the attacker takes different actions during the attack process depending on its policy ($P$).



1-4244-0270-0/06/$20.00 (c)2006 IEEE

*This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2006 proceedings.*

In our model, if $P$ is low, then the attacker will give preference to rapidly compromising sensor network performance (minimizing $AC$). On the other hand, if $P$ is high, then the attacker will give preference to preserving the deployment field (minimizing $DC$). As such, the parameter $P$ becomes a knob that can control attack impacts on $AC$ and $DC$.

We conduct a detailed performance measurement of policy-driven physical attacks in sensor networks through simulation. We observe that the policy parameter $P$ has significant impacts on the network performance $AC$ and destruction casualty $DC$, demonstrating the fact that the attacker can achieve desired bias in its objectives. Our data show that the sensitivities of $AC$ and $DC$ are also related to the attacker parameters (namely, signal detection accuracy and speed of destruction), apart from $P$.

Physical attacks are patent and potent threats to future sensor networks. We believe that viability of future sensor networks is contingent on their ability to resist physical attacks. As such, our work is an important step in this regard. The rest of the paper is organized as follows. In Section II, we first discuss the classification of physical attacks in sensor networks and related sensor network features. We present our policy-driven physical attack model in Section III. In Section IV, we report our performance measurement data. We discuss important related work in Section V. Finally, we conclude our work in Section VI.

## II. Background

In this section, we will discuss the features of sensor networks that can be taken advantage by the physical attacks and the classification of physical attacks in sensor networks.

### A. Sensor Networks

A sensor network is composed of a large number of sensors, which consists of sensing, data processing, and communicating components to fulfill the task decided by the application requirement. The small form factor of the sensors makes them vulnerable to physical destruction. Furthermore, the sensors are usually randomly deployed and unattended, thus will not be recovered once destroyed or damaged. The communication among sensors are through wireless radio, which can be detected by anti-sensor forces and used to locate the sensors. The circuits of active sensors might also emit other detectable signals except radio signals.

We classify sensor signals that can be detected by the attacker into two types, namely *Passive* signals and *Active* signals. Passive signals include heat, vibration, magnetic signals etc., which are part of the physical characteristics of the sensors[1]. Active signals on the other hand include communication messages, beacons, query messages etc., which are part of normal communications among sensors in the network. The attacker can detect both passive and active signals to identify sensor locations. However, the distance within which an active signal can be detected is larger than the distance for detecting a passive signal because the active signal can propagate larger distance.

[1]In this paper, we assume that the attacker is not able to visually identify sensors or the sensors are camouflaged.

### B. Physical Attacks in Sensor Networks

Physical attacks are those attacks that result in the physical destruction of the sensors, rendering them permanently non-operational. A wide spectrum of physical attacks is possible in the domain of sensor networks. Broadly speaking, the spectrum of physical attacks can be considered to operate in two phases, namely the *targeting* phase and the *destruction* phase. In the targeting phase, the attacker tries to identify the sensors or the deployment area of the sensor network. Then, the destruction phase follows to destroy the sensors. As such, we classify physical attacks into the following two types.

*Blind Physical Attacks:* In blind physical attacks, the execution of the targeting phase is to just identify the sensor deployment field. Following this, the deployment field is attacked using a brute-force approach to physically destroy the sensors. Typical brute-force physical attacks occur in the form of bombs/grenades dropped in the field, tanks/vehicles driven around destroying contiguous portions of sensors in the field etc. Sensors that happen to be in the vicinity of attacked areas are simply destroyed.

*Search-based Physical Attacks:* Here the attacker first searches for sensors in the network by detecting signals emitted by the sensors using appropriate signal detecting equipment. After the detection, the attacker destroys the identified sensors physically. Destruction of the small size sensors is typically accomplished through elaborate physical force, radiation and other hardware/circuit tampering techniques that in effect destroy the physical hardware. In many situations, if the attacker wishes to conduct physical attacks, blind (brute-force destructions) attacks may be infeasible. For instance, in some cases it may be necessary for the attacker to preserve the field of interest (like airports, oil fields, battlefields) that are of interest to the attacker. Destroying such areas by means of grenades or bombs will cause destruction of the field. In such cases, the attacker will indulge in search-based physical attacks to identify/detect sensors and destroy only the detected sensors.

Physical attacks do share some similarities with attacks that attempt to compromise the physical features of the sensor to prevent them from providing service [3]. The specific type of attack most related to physical attacks is jamming attacks [3], [4], [5], where the attacker jams or interferes with the radio frequencies that node(s) are using. For networks operating on a single frequency, this attack is simple to launch and highly destructive. However, jamming attacks may be complicated to launch, when there are multiple frequencies of operation. Also, attack related communications in the network can be compromised under jamming attacks. Physical attacks are quite different from jamming attacks in that jamming only causes a loss of operation for the attack duration, while physical attacks result in irreversible sensor destructions. Another difference is that there is a searching process in search-based or policy-driven physical attacks which is not the case in jamming attacks. Furthermore, the standard defense for jamming attacks, namely using forms of spread-spectrum communication [4] cannot be used to defend against physical attacks, as the attacker just needs raw signals to detect sensors.

## III. Modeling Policy-driven Physical Attacks

In this section, we will discuss the policy-driven physical attack model from the perspective of (i) attacker objectives, (ii) attacker capacities, (iii) attack procedure and (iv) attack action control.

### A. Attacker Objectives and Model Metrics

The first objective of the attacker is to identify and destroy sensors with the intention of compromising sensor network performance. We define a novel performance metric in this paper, namely *Accumulative Coverage (AC)*. $AC$ is defined as the integration of the network coverage over the *effective lifetime* of the sensor network. Network coverage is defined as the percentage of the sensor field that is in the sensing range of at least one active sensor [2]. Denoting *coverage(t)* as the network coverage at time $t$, and $EL$ as the effective lifetime, we have,

$$AC = \int_{t=0}^{EL} coverage(t)dt. \quad (1)$$

We believe that $AC$ is an effective metric to measure the performance of a sensor network in many situations since it effectively combines both coverage and lifetime, two important performance metrics in sensor networks. Effective lifetime ($EL$) is defined as the maximum time period during which the coverage is above a certain threshold $\alpha$ (that is system desired). $EL$ considers coverage, but it is not representative enough for situations where for the same effective lifetime, a sensor network with a higher coverage can provide more accurate information than one with a lower coverage. Our metric in this paper, $AC$ considers both coverage and lifetime, and is hence representative of real-life situations. The degradation of $AC$ measures the effectiveness of the search-based physical attacks because one important objective of the attacker is to compromise sensor network performance.

The other objective of the attacker is to minimize the attack casualties to the sensing field if the attacker attempts to preserve the interest of the sensing field. We define a metric, namely *Destruction Casualty (DC)*. $DC$ is the accumulation of the destructed areas in the physical attacks and represents the accumulative attack casualties to the sensing field. If the attacker attacked a set of $n$ sensors $K = \{S_1, \ldots, S_n\}$, and the destroyed area for sensor $S_i$ is $D_i$, then

$$DC = \bigcup_{S_i \in K} D_i. \quad (2)$$

### B. Modeling the Attacker Capacities

We now discuss the capacities of the attacker in our policy-driven physical attack model.

*1) Signal Detection and Sensor Isolation:* The features characterizing this action include, target of search, method of search and capacity of search. In our model, the target can be normal sensors or cluster-heads.[3] While the attacker can detect multiple sensors, the *target* denotes the particular sensor that the attacker currently chooses to destroy. The searching method used by the attacker is by detecting passive and active signals emitted by sensors. The search capacities of the attacker are the distance within which signals can be detected (also called detection range) and detection accuracy.

We denote $R_{ps}$ as the maximum distance within which the attacker can detect a passive signal (for both normal sensors and cluster-heads). We denote $R^s_{as}$ as the maximum distance within which the attacker can detect an active signal emitted by a normal sensor, and $R^h_{as}$ as the maximum distance within which the attacker can detect an active signal emitted by a cluster-head. Since cluster-heads send out higher strength active signals, we have $R^s_{as} < R^h_{as}$. Since, passive signals are detectable from smaller ranges compared to active signals, we also have $R_{ps} < R^s_{as} < R^h_{as}$.

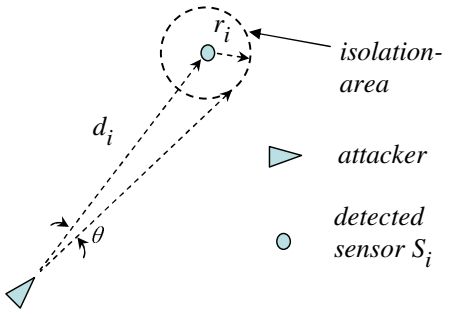



Fig. 1. The isolation-area of the detected sensor.

The second parameter to model signal detection capacity is the detection accuracy. Once a signal from a sensor (say $S_i$) is detected, the attacker will attempt to locate the sensor ($S_i$). To do this, the attacker needs to estimate the distance ($d_i$) from its current position to the sensor, and the orientation or the arrival angle of the detected signal [6], [7]. The attacker can only isolate the sensor's location within a certain area because its estimation of the sensor's location is not accurate. The area isolated can be modeled as a circle with radius $r_i$ and the center of the circle is the estimated location of the detected sensor as shown in Fig. 1. In order to determine $r_i$, the attacker will make use of the maximum detection error, $\theta$, when it detects the orientation of the received signal [6], [7] and the estimated distance of the signal source (sensor $S_i$) as follows,

$$r_i = d_i \times \sin(\theta). \quad (3)$$

We can see that the accuracy of the attacker in determining the sensors location is inversely proportional to $\theta$. That is, if $\theta$ is small, $r_i$ is small, the isolation area is small, which means the accuracy of detection/isolation is high. Hence, we use $\theta$ to measure the detection accuracy of the attacker. We call the area (the size of which is $\pi r_i^2$) as the *isolation-area* for sensor $S_i$. The attacker knows that the detected sensor is in the isolation-area but it does not know the exact location of the sensor. Thus, the attacker will proceed to attack whole of this area with the certain destruction method if it wants to destroy this sensor.

When the attack has not detected any sensor, it walks

[2] We consider 1-coverage in this paper.

[3] We assume that the base station is well protected and cannot be reached or destroyed by the attacker, and thus is not the target of the attacks.

randomly while performing searching. We denote $v_{mv}$ as the average movement speed of the attacker. In our model, the attacker is equipped with memory to store locations of sensors. If the attacker detects multiple signals, it will store the estimated locations of the signal sources and the corresponding isolation-areas in memory. We also assume that the attacker has the ability to detect boundaries of the sensor network, and can hence stay within the network area as long as it is attacking the network.

*2) Sensor Destruction Methods:* There are two methods used by the attacker to physically destroy sensors after the attacker identifies the corresponding isolation-areas of the sensors. The first method is referred to as *sweeping*, in which the attacker can *sweep* the isolation-area by means of *sweeping* using radiation, or with other hardware/circuit tampering techniques, or by applying physical force. Sweeping destruction method is slow. The attacker needs to move to, and reach the isolation-area first, then sweep the whole isolation-area. However, sweeping destruction method is accurate in terms of destruction area and only causes damage to the isolation-area thus introduces minimal casualty to the sensing field.

The second destruction method is referred to as *bombing*, in which the attacker can *bomb* the isolation-area by means of brute-force approaches in the form of bombs/grenades dropped in the area. The attacker does not need to reach the target when it uses bombing to destroy the target sensor. Bombing is quick but inaccurate in terms of the destruction area/location. Each bombing attempt damages a certain area and it is hard to accurately limit all the damage within the isolation-area, especially when the bombing is remotely issued. Thus, the damaged area by bombing is larger than the isolation-area and it contains the isolation-area.

Bombing destruction method is not accurate in terms of destruction area and incurs extra casualty (larger destruction area) to the sensing field. However, bombing does not require the attacker to reach the isolation-area and is fast in destroying sensors.

### C. The Policy-driven Physical Attack Model Procedure

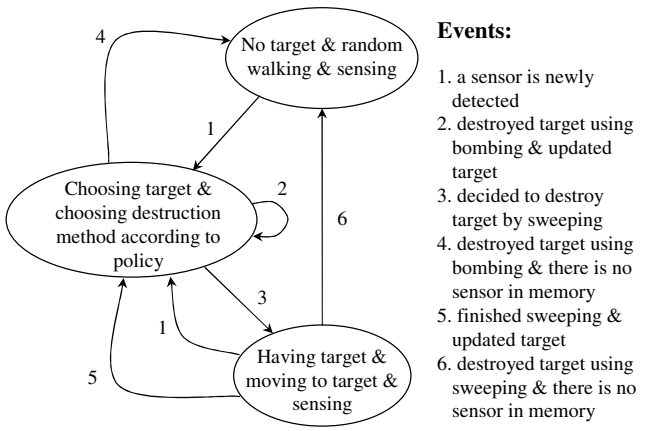



Fig. 2. The procedure of policy-driven physical attack.

In this subsection, we describe the attack procedure of the policy-driven physical attack model, which is shown in Fig. 2. The attack procedure is primarily state/event driven. That is, the attacker is in one state at anytime, and switches among states responding to different events in the network, depending on the types of the events occurred.

At the start in the attack procedure, the attacker does not have any detected sensor to destroy (*State: No target & random walking & sensing*), i.e., the attacker has no *target*. Here, the attacker performs a random straight line walk in the network field and keeps detecting signals. Once the attacker detects one or more signals (*Event: a sensor is newly detected*), the attacker identifies one or more sensors. While the attacker has only one detected sensor, the attacker will set this sensor as the target. However, when multiple sensors are detected, or when a new sensor is detected during moving to current target (*Event: a sensor is newly detected*) when the attacher is in *State: Having target & moving to target & sensing*, or when the attacker has multiple detected sensors in memory and it has just finished destroying a target (*Event: destroyed target using bombing & updated target* or *Event: finished sweeping & updated target*), the attacker chooses the nearest detected sensor as the target. Whenever the *target* is chosen (*State: Choosing target & choosing destruction method according to policy*), the attacker will select a sensor destruction method and take further action according to the policy-based attack action control approach (which is discussed in the following subsection). If bombing destruction method is selected, the attacker will start to destroy the target by bombing the corresponding isolation-area of the target. If sweeping destruction method is selected, the attacker will switch to *State: Having target & moving to target & sensing* and will move to the target and destroy the target by sweeping the corresponding isolation-area after it reaches the isolation-area. Whenever the target is destroyed and there is no detected sensor in the memory (*Event: destroyed target using bombing & there is no sensor in memory* or *Event: destroyed target using sweeping & there is no sensor in memory*), the attacker switches to the initial state (*State: No target & random walking & sensing*).

### D. Policy-based Attack Action Control

We now discuss how the attacker controls its action based on the policy. Recall that the policy represents the *bias* between the twin objectives of the attacker rapidly destroying sensors ($AC$), and minimizing casualties to the deployment field ($DC$). In our attack model, the bias is achieved by choosing the appropriate method of sensor destruction whenever a sensor is chosen as a target by the attacker. We now discuss how the destruction method is dynamically chosen for each targeted sensor depending on the attacker policy.

There are two methods of sensor destruction in our attack model. The *Bombing* method is one where in each bombing instance, the area destroyed is large. Many sensors die and consequently $AC$ decreases fast. The *Sweeping* method for destruction is one, where a very small area around the sensors is destroyed, and as such the casualty to the deployment field is minimal, but the decrease in $AC$ is not fast. In our attack model, for each target sensor, the attacker will evaluate the impacts of $AC$ and $DC$ if the target sensor is destroyed.

Depending on the above impacts and the attacker's policy, the attacker will choose either bombing or sweeping method to destroy the targeted sensor. In the following, we discuss the quantification of the impacts on $AC$ and $DC$ for target sensor $S_i$ using sweeping and bombing, and the selection of destruction method respectively.

*1) Impact of Sweeping and Bombing on $DC$ :* The destruction casualty caused by destruction of $S_i$ with these two destruction methods can be measured by the destruction areas caused by sweeping and bombing method, $D_i^{sw}$ and $D_i^{bo}$ respectively. The sweeping destruction area, $D_i^{sw}$ is $\pi r_i^2$, which is exactly equal to the isolation-area for $S_i$. Thus,

$$D_i^{sw} = \pi r_i^2. \tag{4}$$

While sweeping destruction method is slow, it is accurate in terms of destruction area thus introduces minimal casualty to the sensing field.

On the other hand, bombing destruction method is not accurate in terms of destruction area and incurs large casualty (larger destruction area) to the sensing field. If the isolation-area radius is $r_i$, we model the destruction area due to bombing as a circle with a radius $r_i + R_{be}$, where $R_{be}$ is the bombing area error margin which represents the extra casualty (extra destruction area) caused by the less-accurate bombing. Thus,

$$D_i^{bo} = \pi(r_i + R_{be})^2. \tag{5}$$

*2) Impact of Sweeping and Bombing on $AC$:* The impact of destruction of a sensor (say $S_i$) on $AC$ can be measured by how fast the attacker destroys $S_i$, i.e., how fast the coverage contributed by $S_i$ is compromised. We denote $T_i^{sw}$ and $T_i^{bo}$ as the time spent to destroy sensor $S_i$ using sweeping and bombing destruction methods respectively. Irrespective of the destruction method, the coverage loss is same, which is the coverage provided by $S_i$. We discuss the calculation of $T_i^{sw}$ and $T_i^{bo}$ below.

Denoting $v_{sw}$ as the *sweeping speed*, i.e., the size of area that the attacker can sweep per second, and $r_i$ as the isolation-area radius for sensor $S_i$, we have the time ($t_i^{sw}$) taken to sweeping this isolation-area as,

$$t_i^{sw} = \pi r_i^2 / v_{sw}. \tag{6}$$

Using sweeping destruction method, the attacker needs to move to reach the isolation-area first. The time taken to move to the isolation-area is,

$$t_i^{mv} = d_i' / v_{mv}, \tag{7}$$

where $d_i'$ is the distance from the current location (at the moment when the attacker determines the destruction method) of the attacker to the isolation-area. Then the total time taken to destroy sensor $S_i$ using sweeping, denoted as $T_i^{sw}$, is,

$$T_i^{sw} = t_i^{sw} + t_i^{mv} = \pi r_i^2 / v_{sw} + d_i' / v_{mv}. \tag{8}$$

Recall that if the isolation-area radius of sensor $S_i$ is $r_i$, we model the destruction area caused by using bombing method ($D_i^{bo}$) as a circle with a radius $r_i + R_{be}$. Denoting $R_b$ as the radius of the area (a circle) destroyed by one bombing destruction attempt, $\mu$ as the bombing rate, i.e., the number of bombing attempts the attacker can issue to one isolation-area in one second, we have the time to destroy the isolation-area using bombing ($t_i^{bo}$),

$$t_i^{bo} = \frac{D_i^{bo}/\pi R_b^2}{\mu} = \frac{\pi(r_i + R_{be})^2/\pi R_b^2}{\mu}. \tag{9}$$

The total time to destroy $S_i$ using bombing, $T_i^{bo} = t_i^{bo}$ as the attacker does not need to move to $S_i$, and $T_i^{bo}$ is only the time spent to bomb the destruction area $D_i^{bo}$.

*3) Selection between Sweeping and Bombing :* Now the issue is how to combine the two objectives together based on the policy, i.e., how to combine the impacts of destruction of $S_i$ on $AC$ and $DC$ together while considering the bias (decided by the policy) given to the two objectives in the selection of destruction method. For the destruction of sensor $S_i$, if we set the bias given to the objective of minimizing $AC$ to be 1, and refer to the relative bias given to the objective of minimizing $DC$ as $P$, then the combined impacts to $AC$ and $DC$ considering their biases using bombing and sweeping can be modeled as,

$$F^{bo}(i) = T_i^{bo} \times (D_i^{bo})^P, \tag{10}$$

and

$$F^{sw}(i) = T_i^{sw} \times (D_i^{sw})^P, \tag{11}$$

respectively. Bombing destruction method will be chosen if $F^{bo}(i) \leq F^{sw}(i)$, otherwise sweeping will be chosen by the attacker.

Thus, $P$ is a knob to fulfill the policy of the attacker during the attack. The value of $P$ is set by the attacker based on its policy on preserving the sensing field. In the extreme case when $P$ is infinity, the attack is search-based attack as we modeled in [2]. In the extreme case when $P$ is zero, the attacker's policy does not require to preserve the sensing field, and it always uses brute-force bombing to destroy detected sensors because usually bombing is faster than sweeping.

## IV. Performance Measurement

In this section, we report our performance measurement of the impacts of policy-driven physical attacks on sensor networks. Our performance metrics here are Accumulative Coverage ($AC$) and Destruction Casualty ($DC$), and the policy-driven attack model is the one described in Section III. We will study the impacts of different policies and attacker features to $AC$ and $DC$ under policy-driven physical attacks.

### A. Measurement Environment

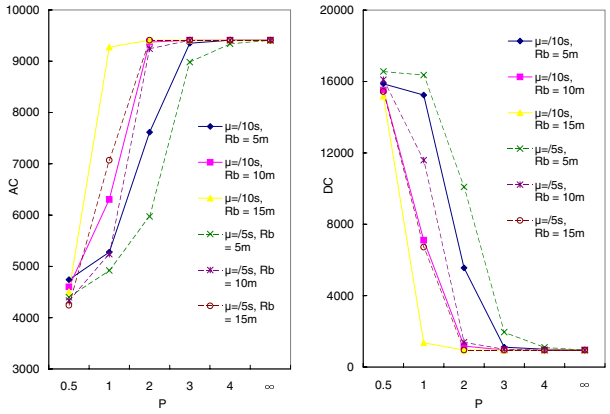
Our sensor network is a field of size $500\ m \times 500\ m$. In the field, $1000$ sensors are randomly uniformly deployed. Sensors emit active signals with a rate denoted as $f$. Each cluster has a cluster-head to which all its children sensors send data. Sensors rotate among themselves to periodically elect new cluster-heads with average rate of $\frac{1}{600\ s}$. The attacker initially performs a random straight line walk in the network searching for sensors.

Unless otherwise stated, following are the default values of specific sensor network and attacker parameters used in the

simulations. Active signal frequency, $f = \frac{1}{30\ s}$; passive signal detection range, $R_{ps} = 1\ m$; active signal detection range of cluster-heads, $R^h_{as} = 50\ m$; active signal detection range of non-cluster-head sensors, $R^s_{as} = 20\ m$; detection error of the signal arrival angle, $\theta = 0.1 radian$; attacker moving speed, $v_{mv} = 0.5\ m/s$; attacker sweeping speed, $v_{sw} = 0.25\ m^2/s$; bombing attack rate, $\mu = \frac{1}{10\ s}$; radius of each bombing, $R_b = 5\ m$; bombing area error margin, $R_{be} = 2\ m$; minimal coverage requirement of the sensor network, $\alpha = 50\%$ ($\alpha$ is used in determining Effective Lifetime ($EL$) and $AC$). Each point of data in the following figures is the average of results from simulations on 5 different random network topologies.

### B. Performance Results

We first report data to highlight the sensitivities of sensor network performance ($AC$) and attack casualty ($DC$) to $P$, which represents the policy of the attacker, i.e., the relative bias the attacker gives to the objective to preserve the sensing field, under different bombing destruction capacities. We then report data to show the sensitivities of $AC$ and $DC$ to $P$ with different sweeping destruction capacities.



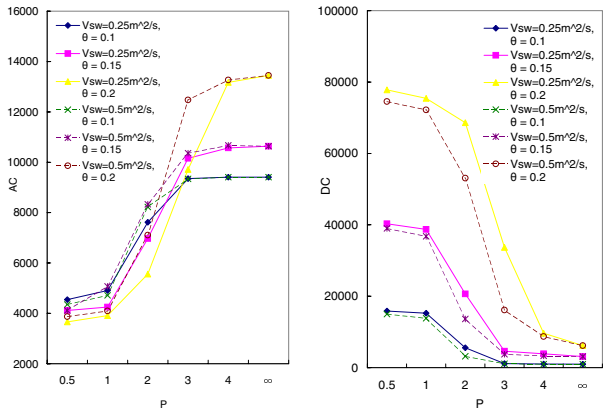

(a) (b)

Fig. 3. Sensitivities of $AC$, $DC$ to $P$ with different $\mu$, $R_b$.

*1) Sensitivities of AC and DC to P under different bombing destruction capacities:* Fig. 3 (a) and (b) show how policy $P$ impacts $AC$ and $DC$ respectively, under varying bombing destruction capacities, i.e. the rate of bombing ($\mu$) and the destruction area radius of one bombing destruction attempt ($R_b$). We make following important observations from these two figures. The first observation is, $P$ significantly impacts $AC$ and $DC$. When $P$ increases, $AC$ is increased and $DC$ is decreased. This illustrates that the attacker can effectively achieve its bias between the two objectives, minimizing sensor network performance (minimizing $AC$) and preserving the sensor network deployment field (minimizing $DC$). Larger $P$ means more bias to preserving the sensor network deployment field. When $P$ is larger enough ($P \geq 4$), bombing is seldom used and the bombing capacities ($R_b$ and $\mu$) have little impact to $AC$ and $DC$ as shown in the figures.

The second observation is, $\mu$ impacts $AC$ and $DC$ significantly. When $\mu$ is increased, bombing is faster, then $AC$ is decreased. When $\mu$ is larger, the bombing destruction time ($T^{bo}_i$) is smaller for any given sensor target $S_i$, bombing destruction has more chances to be selected, thus $DC$ is larger.

The third observation is, $R_b$ also impacts $AC$ and $DC$ significantly. However, the sensitivities of $AC$ to $R_b$ is significantly impacted by $P$. If the attacker has little interest to preserve the sensing field ($P = 0.5$), when $R_b$ increases, $AC$ is decreased. However, when $P$ is not very small, the attacker also cares about how to reduce $DC$. In this situation, when $R_b$ increases, more chances are given to sweeping destruction instead of bombing, thus $AC$ is increased.




(a) (b)

Fig. 4. Sensitivities of $AC$, $DC$ to $P$ with different $v_{sw}$, $\theta$.

*2) Sensitivities of AC and DC to P under different sweeping destruction capacities:* Fig. 4 (a) and (b) show how $P$ impacts $AC$ and $DC$ respectively, under varying attacker sweeping speed ($v_{sw}$) and detection accuracy ($\theta$). The time to finish sweeping destruction is impacted by $v_{sw}$, which is shown in Formula (8). From Formula (3) and (8), we can see that $\theta$ impacts the time to sweep through its impact on $r_i$. We observe that the sensitivities of $AC$ and $DC$ to $P$ are impacted by $v_{sw}$ and $\theta$ significantly. The first observation we make is that, $P$ control the tradeoff between minimizing $AC$ and minimizing $DC$ flexibly as explained in Section IV-B.1.

The second observation is, when $\theta$ increases, $DC$ is increased due to larger isolation-areas as shown in Fig. 4 (b). However, the sensitivity of $AC$ to $\theta$ is impacted by $P$. As shown in Fig. 4 (a), when $P$ is large, more destructions are through sweeping. In this situation, larger $\theta$ means more time cost on slow sweeping (larger isolation-areas), thus $AC$ is larger. But when $P$ is small, the attacker cares more on how to reduce $AC$ fast. In this situation, larger $\theta$ (means larger isolation-areas and larger sweeping time) gives more chances to bombing destruction, hence the coverage is degraded faster and $AC$ is smaller.

The third observation is, when $v_{sw}$ increases, $AC$ is increased and $DC$ is decreased. The reason is, when $v_{sw}$ is larger, sweeping is faster thus will have more chances to be selected to destroy sensors. Hence $AC$ is larger and $DC$ is smaller because sweeping is usually slower and causes less casualty compared with bombing destruction.

## V. Related Work

Security in WSNs is a broad area. We highlight work most related to our study here. A good overview of current status in security and research issues is presented by Perrig et al. in [8]. Some of the security concerns include resilient routing, secure communication, and electronic and physical node destructions. In [9], Karlof and Wagner, present a survey on sensor network routing protocol vulnerabilities and defense schemes against several electronic attacks. Two of these attacks are the Sybil attack [10] and the wormhole attack [11]. In [12], Newsome et al. further analyze the Sybil attack and show that it has several variants that affect data aggregation, voting, misbehavior. They also develop effective defense mechanisms against these different attack variants. In [13], Hu et al. investigate the wormhole attack and propose packet leashes to prevent an attacker from maliciously tunneling packets to different areas in a WSN. Taking another approach to routing in security, Deng et al. propose INSENS, intrusion tolerant routing that detects malicious sensors and routes around them [14]. Some of the concepts in [14] were taken from [15] which provides two security protocols, SNEP and $\mu$TESLA. These protocols insure data confidentiality, authentication, freshness and authenticated broadcast in severely resource constrained environments like WSNs, and provide defense to Sybil attack, wormhole attack, eavesdrop attack [16], [8], [17], spoof, reply and message alter attack [9].

In [18], attackers perform traffic analysis on the messages transmitted to the base station to determine its location. A host of attacks can now be orchestrated if the base station can be determined accurately, including jamming attacks [3], eavesdropping attacks, Sybil attacks etc. In [18] and [19], approaches to protecting the base station are discussed.

Denial-of-service (DoS) attacks are another key area of vulnerability and research in WSNs. Wood and Stankovic study the threat at different layers in the network [3]. They also present design time factors that, if taken into consideration, reduce network vulnerability to DoS attacks. In [5], they further develop the radio-frequency jamming DoS attack and present a technique to route around the jammed area.

Another recent work is Patil's work in [20]. Here the author discusses the end effects of physical node destructions. Our work here in fact proposes a model for such attacks that cause node destructions. The metrics used in [20] is coverage and connectivity, while ours are Accumulative coverage ($AC$) and Destruction Casualty ($DC$).

In some cases, attackers can compromise sensors with malicious intent. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker etc. To protect against tampering with the sensors, one defense involves tamper-proofing the node's physical package [3]. Another class of work like [21] focuses on building tamper-resistant hardware in order to make the actual data and memory contents on the sensor chip inaccessible to attackers.

Across some respects, the end effects of physical attacks are similar to fail-stop fault models [22], [23], where the sensor is simply dead. However in physical attacks, the node destructions are orchestrated by an attacker. Also the faults (dead sensors) are not independent or isolated. Rather, they have geographical similarities. In search-based or policy-based attacks, the distribution of dead nodes are related to the motion of the sensor-searching attacker. This changes the problem in that previously proposed purely fail-stop models are no longer applicable under the presence of a sensor-searching attacker.

Physical attacks are different from a host of sensor network attacks proposed in the literature. Physical attacks destroy sensors permanently. The losses are irreversible, unlike many other attacks, where the sensors are not physically destroyed and hence are recoverable. In a prior work, we have identified and modeled blind physical attacks [1]. In [1], we studied the issue of deployment of sensors in a sensor network to meet lifetime requirement under blind physical attacks. In [2], we modeled the search-based physical attacks and analyzed the impacts of search-based physical attack on sensor network performance. Our focus in this paper is policy-based physical attacks, which combines the merits of blind attacks and search-based attacks and achieves an expected bias between the objectives of the attacker to minimize the sensor network performance and to minimize the attack casualty to the sensor network deployment field.

## VI. Conclusions

In this paper we addressed the issue of physical attacks in sensor networks. Specifically, we first discussed the classification of physical attacks into blind and search-based attacks, and identified their critical features. We then modeled and analyzed policy-driven physical attacks, where the bias between the twin objectives of the attacker (rapidly destroying sensors, and preserving the deployment field) is modeled as a policy for the attacker. Our performance data clearly showed that the attacker policy has impacts on accumulative coverage ($AC$) and destruction casualty ($DC$), demonstrating that the attacker can achieve desired bias in its objectives under *policy-driven physical attacks*.

To the best of our knowledge, ours is the first work that identifies the problem and models policy-driven physical attacks. We however believe that this is just one of the first steps in this regard. There are other open issues in this subject. Our current on-going is focusing on modeling other variants of physical attacks. We are specifically focusing on modeling multiple physical attackers cooperating among themselves. The orthogonal dimension of defending against physical attacks is also a part of our on-going work.

## References


[1] X. Wang, W. Gu, S. Challeppan, K. Schoseck, and D. Xuan, "Lifetime optimization of sensor networks under physical attacks," in *Proc. of IEEE Internationl Conference on Communications (ICC)*, May 2005.

[2] X. Wang, S. Chellappan, W. Gu, W. Yu, and D. Xuan, "Search-based physical attacks in sensor networks," in *Proc. of International Conference on Computer Communications and Networks (ICCCN)*, October 2005.

[3] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, no. 10, pp. 54–62, October 2002.

[4] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley Computer Publishing, March 2001.

[5] A. D. Wood, J. A. Stankovic, and S. H. Son, "Jam: A jammed-area mapping service for sensor networks," in *Proc. of Real-Time Systems Symposium (RTSS)*, December 2003.
[6] N. B Priyantha, A. Miu, H. Balakrishnan, and S. Teller, "The cricket compass for context-aware mobile applications," in *Proc. of the International Conference on Mobile Computing and Networking (MobiCom)*, July 2001.
[7] D. Niculescu and B. Nath, "Ad hoc positioning system (aps) using aoa," in *Proc. of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, April 2003.
[8] A. Perrig, J. Stankovic, and David W., "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–75, June 2004.
[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. of 1st IEEE International Workshop on Sensor Network Protocols and Applications (SNPA)*, May 2003.
[10] J. R. Douceur, "The sybil attack," in *Proc. of 1st International Workshop on Peer-to-Peer Systems (IPTPS)*, March 2002.
[11] Y. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Tech. Rep. TR01-384, Department of Computer Science, Rice University, June 2002.
[12] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis and defenses," in *Proc. of 3rd International Symposium on Information Processing in Sensor Networks (IPSN)*, April 2004.
[13] Y. Hu, A. Perrig, and David B. J., "Packet leashes: A defense against wormhole attacks in wireless ad hod networks," in *Proc. of 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, April 2003.
[14] J. Deng, R. Han, and S. Mishra, "Insens: Intrusion-tolerant routing in wireless sensor networks," in *Proc. of IEEE International Conference on Distributed Computing Systems (ICDCS)*, May 2003.
[15] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," in *Proc. of 7th Annual International Conference on Mobile Computing and Networking (MobiCom)*, July 2001, pp. 188–199.
[16] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. of 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, March 2004.
[17] S. Zhu, S. Setia, and S. Jajodia, "Leap: Efficient security mechanisms for large-scale distributed sensor networks," in *Proc. of the 10th ACM Conference on Computer and Communications Security (CCS)*, October 2003.
[18] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *Proc. of the IEEE International Conference on Dependable Systems and Networks (DSN)*, June 2004.
[19] J. Deng, R. Han, and S. Mishra, "Enhancing base station security in wireless sensor networks," Tech. Rep. CU-CS 951-03, Department of Computer Science. University of Colorado, November 2002.
[20] S. Patil, "Performacne measurement of ad-hoc sensor networks under threats," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, March 2004.
[21] R. J. Anderson and M. G. Kuhn, "Low cost attacks on tamper resistant devices," in *Security Protocols – Proc. of the 5th International Workshop*, April 1997.
[22] F. B. Schneider, "Implementing fault-tolerant services using the state machine approach: A tutorial," *ACM Computing Surveys*, vol. 22, no. 3, December 1990.
[23] R. H. Arpaci-Dusseau and A. C. Arpaci-Dusseau, "Fail-stutter fault tolerance," in *Proc. of Workshop on Hot Topics in Operating Systems*, May 2001.