Search-based Physical Attacks in Sensor Networks

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

Abstract— **The small form factor of the sensors, coupled with the unattended and distributed nature of their deployment expose sensors to *Physical Attacks* that physically destroy sensors in the network. In this paper, we study the modeling and analysis of *Search-based Physical Attacks* in sensor networks. We define a search-based physical attack model, where the attacker walks through the sensor network using signal detecting equipment to locate active sensors, and then destroys them. We consider both flat and hierarchical sensor networks. The attacker in our model uses a weighted random selection based approach to discriminate multiple target choices (normal sensors and cluster-heads) to enhance sensor network performance degradation. Our performance metric in this paper is *Accumulative Coverage* (AC), which effectively captures coverage and lifetime of the sensor network. We then conduct detailed evaluations on the impacts of search-based physic attacks on sensor network performance. Our performance data clearly show that search-based physical attacks significantly reduce sensor network performance. We observe that attack related parameters, namely attacker movement speed, detection range and accuracy have significant impacts on the attack effectiveness. We also observe that the attack effectiveness is significantly impacted by sensor network parameters, namely the frequency of communication and frequency of cluster-head rotation. We believe that our work in this paper on modeling and analyzing search-based physical attacks is an important first step in understanding their overall impacts, and effectively defending against them in the future.**

I. Introduction

A critical component of on-going research in Wireless Sensor Networks (WSN) is the security of the sensor networks. Research in this area has contributed a host of potential attacks in sensor networks and effective defenses against such attacks [1], [2], [3], [4], [5], [6], [7], [8]. It is widely accepted that viability of sensor network applications in the future is closely contingent on the security of the networks.

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 nonoperational. In this paper we model and study a representative class of physical attacks, namely *Search-Based* physical attacks to understand their behavior and impacts.

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 *fatal* in destruction. In the simplest case, the attacker can just drive a vehicle in the sensor field or hurl grenades/bombs in the field and destroy the sensors. A smarter attacker can detect and destroy sensors with stealth by moving across the sensor network. 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.

Our focus in this paper is *Search-based Physical Attacks*. We define search-based physical attacks as those that search for sensors, and then physically destroy them. The searching process is executed by means of detecting electronic, magnetic, heat signals emitted by the sensors. Once sensors are identified, the attacker physically destroys the sensors. This process is opposed to a rather blind or brute force destruction of sensors in the field (using bombs, grenades, tanks etc) that will cause casualties to the deployment field, which the attacker might want to preserve (airports, oil fields, battlefields etc. of interest to the attacker). The salient features of search-based physical attacks come from the ability to search for and then destroy sensors. This improves the efficiency of the attack process, as the attacker can identify and destroy important sensors (cluster-heads, data aggregators etc.). The search-based attacker can cause physical destruction of the sensors while causing minimum casualties to the field of deployment.

In this paper, we model search-based physical attacks in sensor networks. We consider both flat and hierarchical sensor networks. The attacker in our model uses a weighted random selection based approach to discriminate multiple target choices (normal sensors and cluster-heads). The discrimination is due to the attacker's objective of maximizing performance degradation by *efficiently* identifying and then destroying sensors. We then conduct a detailed performance analysis of impacts of search-based physical attacks in sensor networks, under varying attacker and sensor network parameters. Our performance metric in this paper is the *Accumulative Coverage* of the network. Accumulative Coverage captures both the lifetime and coverage and as such is an effective metric to measure performance.

Our performance data clearly show that search-based physical attacks dramatically reduces accumulative coverage, further highlighting the importance of our work. We observe that the attacker parameters, namely attacker's signal detection ranges, accuracy and movement speed, and the sensor network parameters such as the frequencies of sensors' beacons and frequency of cluster-head rotation have significant impacts on attack effectiveness. We also observe that using a hierarchical sensor network has a mixed impact on maintaining AC

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.

0-7803-9428-3/05/$20.00 ©2005 IEEE.

under attacks; on one hand, the compromised cluster-heads (in hierarchical networks) cause decrease in AC significantly; on the other hand however, the existence of cluster-heads with cluster-head rotation can mislead the attacker and make its movements less efficient. We also observe that the impacts of the attacker and sensor network parameters to attack effectiveness interact with each other to affect AC.

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 first step in this regard. The rest of the paper is organized as follows. In Section II, we first introduce physical attacks in sensor networks. We present our search-based physical attack model in Section III. In Section IV, we report our performance evaluation data. We discuss important related work in Section V. Finally, we conclude our work in Section VI.

II. 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 physical force, radiation and other hardware/circuit tampering techniques that in effect destroy the physical hardware.

In [9], we modeled blind physical attacks. There, we studied the issue of deployment of sensors in a network to meet lifetime requirements under blind attacks. In this paper we focus on search-based physical attacks. 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 and destroy only the sensors. Also, search-based attacks are more efficient in that they can identify and destroy only important sensors (cluster-heads, data aggregators etc.) and cause maximum destruction to the network by destroying only these 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 [8]. The specific type of attack most related to physical attacks in jamming attacks [8], [10], 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 the searching process in search-based physical attacks. The standard defense for jamming attacks, namely using forms of spread-spectrum communication [11] cannot be used here as the attacker just needs raw signals to detect sensors.

III. Modeling Search-based Physical Attacks

In this section, we will discuss the search-based physical attack model in detail. The objective of the attacker is to detect and physically destroy sensors in the network to compromise network performance (We define our performance metric subsequently). Modeling search-based physical attacks involves modeling the sensor network properties (from the perspective of signals emitted by the sensors), and modeling the attacker capacity (in detecting signals and utilizing them) in compromising performance. In the following, we first classify signals emitted by sensors that can be detected by the attacker. We then discuss attacker capacities from the perspective of signal detection, movement and sensor destruction methods. Following this will be our detailed search-based physical attack model.

A. Sensor Network 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., that are part of the physical characteristics of the sensors[1]. Active signals on the other hand include communication messages, beacons, query messages etc., that are part of normal communications between 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. We assume destroyed and sleeping sensors do not emit active nor passive signals.

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

In this paper, we model search-based physical attacks in flat and hierarchical networks. When the sensor network is flat, the detectability of active signals or passive signals (by the attacker) are same for all sensors. In a hierarchical network, we model the upper tier sensors (denoted as cluster-heads) as having higher active signal transmission strengths and larger transmission ranges compared to the lower tier normal sensors. Generally speaking, this is due to cluster-heads having to communicate with other cluster-heads, base-station etc., that may be far away from a cluster-head. That is, the attacker can detect active signals emitted by cluster-heads from a larger distance, compared to the distance within which it can detect an active signal emitted by a normal sensor. The detectability of passive signals (due to physical characteristics) is still the same for cluster-heads and normal sensors. The sensors rotate among themselves to periodically elect cluster-heads. We denote the frequency of cluster-head rotation among sensors as μ, which is the reciprocal of the interval between cluster-head elections. The size of the cluster (the average number of sensors in a cluster) is denoted as C. In this paper, we assume the attacker does not have the capability to reach or destroy the base station.

B. Attacker Capacities

We now discuss the capacities of the search-based attacker in our model.

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. 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 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 discuss further below.

The first parameter to model signal detection capacity is the range of detection of passive and active signals. Both types of signals are quite different in terms of their detectability by the attacker. Passive signals are detectable from only small distances. 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 $R_{ps} < R^s_{as} < R^h_{as}$. We emphasize here that the attacker may or may not have the ability to distinguish between normal sensors and cluster-heads. We discuss both scenarios when we present our attack model in Section III-C.2.

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 from its current position to the sensor, referred to as d_i, and the orientation or the arrival angle of the detected signal [12], [13]. Approaches discussed in [12], [13] can be used for this purpose. The attacker can only isolate the sensor's location within a certain area because its estimation of the sensor's location is not accurate. Defining r_i, as the maximum distance between the sensor's actual location and its location estimated by the attacker. The area isolated is a circle with radius r_i and the center of it is the estimated location of the detected sensor. In order to determine r_i, the attacker will make use of the detection error, θ, when it detects the orientation of the received signal [12], [13] and the estimated distance of the signal source (a sensor) as following,

$$r_i = d_i \times \theta. \tag{1}$$

We can see the accuracy of the attacker in determining the sensors location is inversely proportional to θ. That is, if θ is small, the accuracy is higher (r_i is small). Similarly, a large θ means larger r_i, which consequently means less accurate isolation. Hence, we use θ to measure the detection accuracy of the attacker. We call the area ($= \pi r_i^2$) as the *sweeping area* for sensor S_i. The attacker will proceed to sweep this area if it wants to destroy this sensor.

Attacker Movement: The search-based physical attacker is mobile. In the absence of a target, the walk can be random (while performing searching). We denote v_{mv} as the average movement speed of the attacker. If there is only one target, naturally the attacker moves towards it. In our model, if the attacker detects multiple signals, it will store the estimated locations of the signal sources and the corresponding sweeping areas in memory. The memory available to the attacker is large enough in our model to keep all identified locations. When there are multiple targets, the attacker needs to schedule its movement to reach targets efficiently. In our model, this behaviors is captured using the notion of *weights* (discussed in Section III-C) assigned to each detected sensor by the attacker. 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.

Sensor Destruction Methods: The method used by the attacker to physically destroy sensors can be by means of applying physical force, radiation or other hardware/circuit tampering techniques. Recall that the attacker identifies a sweeping area for destruction. Denoting v_{sw} as the *sweeping speed*, i.e. the size of area that the attacker can sweep per second, and B_i as the sweeping area for sensor S_i, we have the time taken for sweep (t_i^{sw}) of this sweeping area as,

$$t_i^{sw} = \frac{B_i}{v_{sw}}. \tag{2}$$

In our model, the attacker has to physically reach sensors to destroy them. The attacker does not have the capacity to launch remote destruction of sensors.

C. Description of the Search-based Physical Attack Model

1) Attacker Objective: The objective of the attacker is to identify and destroy sensors with the intention of compro-

mising 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], and effective lifetime is the time period until when the sensor network becomes nonfunctional because the coverage falls below a certain threshold α (that is system desired). Denoting *coverage(t)* as the network coverage at time t, and EL, as the effective lifetime, we have,

$$AC = \int_{t=0}^{EL} coverage(t)dt. \quad (3)$$

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 of the most important performance metrics in sensor networks. Effective lifetime is defined as the maximum time period during which the coverage is above a certain threshold and thus considers both coverage and lifetime. However, 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 its objective is to compromise sensor network performance.

Model 1 Search-based physical attack model

```
Initialization: Target ← Φ; Mem ← Φ;
while the attacker is executing attacks do
  switch type of event
  case detected a sensor S:
    Target = Φ:
      Calculate S.weight; Add S to Mem; Target ← S;
      Target.location ← S.location;
    Target ≠ Φ:
      add S to Mem; Update S_i.weight ∀ S_i ∈ Mem;
      Randomly choose S' ∈ Mem and the chance to
        choose S_i is proportional to S_i.weight;
      Target ← S'; Target.location ← S'.location;
  case reached Target.location:
    Destroy Target;
  case finished the destruction of Target:
    Remove Target from Mem;
    Update S_i.weight ∀ S_i ∈ Mem;
    Randomly choose S' ∈ Mem and the chance to choose S_i
      is proportional to S_i.weight;
    Target ← S'; Target.location ← S'.location;
  default:
    Whenever Target ≠ Φ, walk towards Target.location,
      otherwise walk randomly;
  endswitch
end while
```

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

2) The Attack Model: Model 1 describes our search-based physical attack model. The attacker's behavior in the network is primarily event driven. That is, the attacker responds to different events in the network, depending on the event occurred. Broadly, there are three types of events in Model 1. The first is signal detection and choice of a sensor as target. The second is reaching the target and destroying it. The third event is choosing a new target after destruction of the current target. The events are overlapped in time and need not be sequential. An instance is the attacker can detect a signal, while it is moving towards a target.

At the start in Model 1, the attacker does not have any detected sensor to destroy. Here, the attacker performs a random straight line walk (with an average speed v_{mv}) in the network field and keeps detecting signals. Once the attacker detects one or more signals (Event: *detecting a sensor*), the attacker detected one or more sensors. While the attacker has only one detected sensor, the attacker will move towards this target until it reaches the target (Event: *reaching Target location*), and destroy the target. However, when multiple sensors are detected (Event: *detecting a sensor*), or when a new sensor is detected during moving to current target, or when the attacker has multiple sensor locations in memory and it has just finished destroying a target (Event: *finish the destruction of target*), the attacker has to efficiently *choose* the next target.

The issue here is how the attacker should respond when it has multiple detected sensors (normal sensors and cluster-heads), detected by means of active or passive signals, with possibly different times taken to destroy each, in order for the attacker to achieve its objective of compromising AC as much as possible. In this paper, we model the attacker as using a random weighted selection approach to choose one particular sensor as target among multiple detected sensors. We model this using the notion of *weights* assignment for each detected sensor. In this model, the attacker assigns a weight for each detected sensor depending on the time taken to reach and destroy it and its importance (discussed further next) in compromising AC. Once weights are assigned, the attacker randomly chooses a sensor as the target, where the probability of choosing a particular sensor as the target is proportional to the weight of that sensor. That is, larger the weight is for a sensor, higher is the probability that the attacker chooses that sensor as the target.

There can be other approaches to choose targets. One approach is to always choose the sensor with the largest weight as target. Another approach is for the attacker to construct best paths for destroying multiple sensors it has detected. While the above approaches seem to be intuitively reasonable, they are not the best choices for the attacker. Purely choosing targets by decreasing order of weights, may not be best in the long run. In the second approach, the attacker may detect new sensors during destruction, which it may not be able to use efficiently.

3) Weight Determination: The determination of weight for each detected sensor, is a critical component in attacker success. Determination of the weight for a particular detected sensor is related to the following; current distance from the attacker to the detected sensor, whether the sensor is a normal

sensor or a cluster-head, accuracy of isolation of the sensor.

We propose two approaches for determining the weights. The first strategy models attackers that aim to maximize performance degradation by destroying sensors that take less time to destroy (irrespective of whether the attacker's can or cannot distinguish between cluster-heads and normal sensors). An intuitive notion of weight is related to the time taken to reach and destroy a sensor. Let us denote d_i as the estimated distance between the current location of the attacker and the location of a detected sensor S_i [3]. Recall that B_i is the sweeping area for sensor S_i. Let t_i denote the total time taken to reach and destroy sensor S_i. This includes the time to move to sensor S_i and the time to sweep the sweeping area for sensor S_i. We then have,

$$t_i = \frac{d_i}{v_{mv}} + \frac{B_i}{v_{sw}}, \tag{4}$$

where v_{mv} and v_{sw} denote the attacker's movement speed, and sweeping speed respectively (defined in Section III-B).

We then have the weight w_i for sensor S_i as,

$$w_i \propto \frac{1}{t_i}. \tag{5}$$

The second weight approach models the attacker giving importance to cluster-heads if it has the ability to distinguish between cluster-heads and normal sensors. That is if the target is a cluster-head, the weight for the cluster-head is given by,

$$w_i \propto \frac{H}{t_i}, \tag{6}$$

where H denotes the importance of a cluster-head from the attackers perspective. If the attacker has some knowledge of the number of children sensors per cluster-head, then H can be set depending on this value. However, such knowledge is not easy for the attacker to obtain. H can be set as a very large value, this means that the attacker gives high priority to cluster-heads compared to normal sensors.

We emphasize here that calculating weights for sensors in memory is not a one time operation. According to the definition of weight, whenever the attacker moves, the distances to detected sensors are changed, hence the weights of them are changed and need to be updated/recalculated. The frequency with which weights are updated has trade-offs between computational overhead and accuracy of weights. However, the attacker only needs most updated weights of un-destroyed detected sensors when it needs to choose or change target. Thus, weights only need to be updated if one or more of the following events happen; the attacker destroys a target; new sensors are detected; new signals are received for an already detected sensor. The occurrence of any of the above events not only means that the attacker needs to choose or change target, it also means that the number of candidates of target changes or the sweeping area of an already detected sensor should be updated. In our model, the attacker updates weights following equation 4, 5 and 6 when any of above events happens. We now discuss how to update weighs, when new signals are received for a sensor already detected and isolated.

From equation 4, one can observe that the time (t_i) to reach and destroy a sensor S_i is proportional to the sweeping area size. The determination of weight w_i is inversely proportional to the time t_i. We propose an approach by which the attacker can smartly reduce the sweeping area size and save time, when multiple signals are detected for sensor S_i. For each signal received, the area isolated by the attacker for sensor S_i changes. Thus, the attacker has multiple sweeping areas for the same sensor. The attacker can save time for destroying this sensor by sweeping only the *small* area that overlaps with all identified sweeping areas (identified per each signal received) for this sensor. That is, the overlapped area is the new sweeping area for this sensor. The novelty in this approach is that the attacker has minimized the time required to sweep the area in order to destroy this sensor. This will enhance the potency of the attacker, further compromising performance.

We wish to state that our search-based attack model presented here is one representative instance. Our model can be extended to represent a wide spectrum of search-based physical attacks. One extreme case is no searching phase in the attack. The attacker can just use random sweeping in order to destroy sensors. This is similar to blind physical attacks [9]. The other extreme case is for the attacker to destroy *only* specific sensors such as cluster-heads, data aggregators etc. Extending our model in this paper to multiple attackers co-operating among themselves is part of our on-going work.

IV. Performance Evaluations

In this section, we report our performance evaluations of the impacts of search-based physical attacks on sensor networks. Our performance metric here is the Accumulative Coverage (AC), and the search-based attack model is the one described in Section III. We will study the sensitivity of both attacker features, and sensor network features to AC under search-based physical attacks.

A. Evaluation 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. The network can be flat or can be hierarchical and divided into clusters. Each cluster has a cluster-head to which all its children sensors send data. Sensors rotate among themselves to periodically elect new cluster-heads. The attacker initially performs a random straight line walk in the network searching for sensors.

Unless otherwise stated, following are the values of specific sensor network and attacker parameters used in the simulations. Active signal frequency, $f = \frac{1}{30\ seconds}$; cluster size (average number of sensors in a cluster), $C = 10$; passive signal detection range, $R_{ps} = 1\ meter$; active signal detection range of cluster-heads, $R^h_{as} = 50\ meters$; active signal detection range of non-cluster-head sensors, $R^s_{as} = 20\ meters$; detection error of the signal arrival angle, $\theta = 1/10 radian$; attacker moving speed, $v_{mv} = 0.5\ meter/second$; attacker sweeping speed, $v_{sw} = 0.25\ meter^2/second$; minimal coverage requirement of the sensor network, $\alpha = 50\%$ (α is used in

[3]The distance d_i estimated by the attacker for a sensor S_i will change as the attacker keeps moving.

determining effective lifetime and AC). Each point of data in the following figures is the average of results from simulations on multiple different random network topologies.

We consider two attack scenarios in our evaluations. The scenario *PA/H* denotes one where the attacker gives priority to cluster-heads, in which case H can be a very large number (in equation 6). The scenario *PA/NH* denotes one where the attacker does not give priority to cluster-heads or the attacker cannot distinguish cluster-head, in which $H = 1$ in weight calculation.

B. Performance Results

We first report data to study the impacts of search-based physical attacks on sensor network performance under varying attack features. We then report data to study the impacts of search-based physical attacks on AC under varying sensor network features.

1) Sensitive of AC to Attacks under different Attacker Capacities (Attacker Movement Speed, Detection Range and Accuracy): Fig. 1 (a) shows the impacts of attacks on AC with varying attacker movement speed (v_{mv}) under different detection accuracy (θ). We report data for both *PA/H* and *PA/NH* scenarios here. Irrespective of θ and whether cluster-heads are given priority, we can see that as v_{mv} increases, AC decreases. The decrease in AC is very sharp in the left portion of the curve, which represents the transition from no attack to slight increases in attack speed. Beyond a certain point, further increases in v_{mv} does not affect AC significantly. The reason is that when v_{mv} is small, any change in speed distinguishes a static attacker from a mobile attacker considerably. The consequence is a large difference on the attack effectiveness, which causes the steep fall in AC. However, when v_{mv} is large, most of the sensors are destroyed in a short time and the sensor network becomes sparse quickly. Thus increased attacker speeds does not increase the attack effectiveness as much in this case, and the fall in AC is less pronounced.

The second observation is that AC is sensitive to θ, and AC decreases when θ decreases. When θ decreases, the isolation error deceases based on equation 1, and the sweeping area is smaller. Consequently, the attacker can detect sensors more accurately and destroy them faster, naturally compromising AC better.

The third phenomenon we can study from Fig. 1 (a), is the sensitive of AC to whether cluster-heads are given priority (*PA/H*)or not (*PA/NH*). We observe that when θ is large ($\theta = 1/5$), PA/NH compromises AC more compared with PA/H. However, when θ is very small ($\theta = 1/20$), PA/H compromises AC better than PA/NH. When θ is large, the isolation of sensors and cluster-heads is not accurate and the resulting sweeping areas are large. Since the signal detection range of cluster-heads is larger than that of normal sensors ($R^h_{as} > R^s_{as}$), the cluster-heads can be detected far away. Thus, the sweeping areas of cluster-heads are much larger that those of normal sensors (from equation 1). Consequently, giving priority to cluster-heads (*PA/H*) cost significant amount of time for the attacker (from equation 4) to destroy a cluster-head. Thus, when θ is large, giving priority to cluster-heads (*PA/H*) is not beneficial for the attacker. On the other hand, when θ is small, the isolation of sensors and cluster-heads is very accurate and the corresponding sweeping areas are small. Under this situation, *PA/H* is beneficial for the attacker, since it can destroy cluster-heads faster and can compromise AC better.

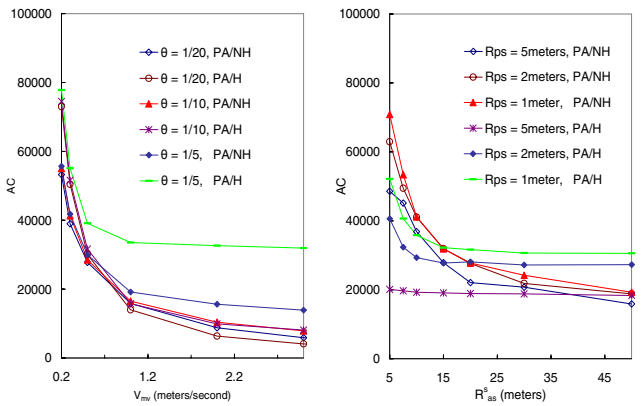

Fig. 1. Sensitivity of AC to attacker capacities, v_{mv}, θ, R^s_{as} and R_{ps}.

Fig. 1 (b) shows the sensitivity of AC to attackers signal detection ranges (R_{ps} and R^s_{as}) under both PA/NH and PA/H scenarios. Irrespective of R_{ps} and PA/NH or PA/H scenarios, we can see that as R^s_{as} increases, AC decreases.

The second observation we make from Fig. 1 (b) is the relationship between R^s_{as}, PA/NH and PA/H scenarios on AC. We observe that, when R^s_{as} is small, PA/H is more effective in compromising AC, and when R^s_{as} is large, PA/NH is more effective. This is because when R^s_{as} is small, the attacker can detect very few nearby normal sensors. In this case, attacking cluster-heads in the local area is more effective to compromise AC. Consequently, PA/H is better for the attacker. When R^s_{as} is large, the attacker can detect many normal sensors within a large range. In this case, giving priority to detected normal sensors (which are many in number) is more effective. Thus, when R^s_{as} is large, PA/NH compromises AC better. The sensitivity of AC to R^h_{as} with different R_{ps} follows a similar pattern and we do not report corresponding performance results.

2) Sensitive of AC to Attacks under different Sensor Network Parameters (Active Signal Frequency, Cluster-head Ratation Frequency and Cluster Size): Fig. 2 (a) shows the impact of attack on AC when cluster-head rotation frequency (μ) changes, with different cluster sizes (C) under both PA/NH and PA/H scenarios. Intuitively speaking, more frequent cluster-head rotation is better under search-based attacks, since destroyed cluster-heads can be replaced faster. Thus, when μ increases, AC increases as we observe in Fig. 2 (a). The second observation here is the relation between the choices of PA/NH and PA/H scenarios with different μ. When μ is small (slower rotation), giving priority to cluster-heads is better, and reduces AC more significantly compared to PA/NH. When μ is larger, cluster-heads are replaced rapidly. In this case, giving priority to cluster-heads is less beneficial for the attacker, hence PA/NH compromises AC more in this case.

The third observation we make is that, when cluster size (C) is small, AC is generally larger. This is because, a small cluster size means, less impacts on AC when the cluster-head is destroyed. From Fig. 2 (a), we can also see the performance trade-offs between flat and hierarchical sensor networks. First, when μ is extreme small (little or no cluster-head replacement), a destroyed cluster-head causes significant loss in AC. Thus, a flat network is better to maintain AC under attacks when μ is very small. Second, when μ is large enough, hierarchical sensor network performs better. The reason is that, when μ is large enough, although the attacker spends significant amounts of time to reach the cluster-heads and destroy them, the cluster-head will be replaced soon. On the other hand, the cluster-head can attract the attacker to spend significant amounts of time in moving to them and destroying them (since cluster-head signals propagate farther than normal sensors and result in larger moving distance and larger sweeping areas according to equation 1).

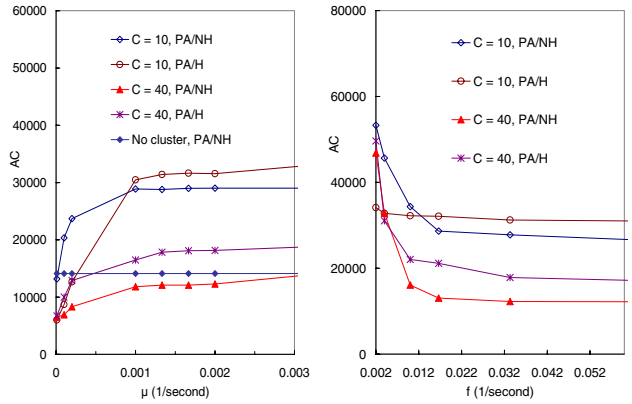

Fig. 2. Sensitivity of AC to sensor network parameters, μ, f and C.

Fig. 2 (b), shows the sensitivity of AC to the active signal frequency (f), under varying cluster sizes (C), under both PA/NH and PA/H scenarios. When f is larger, the attacker can detect more sensors, and consequently AC goes down rapidly. The second observation is that PA/H compromises AC better than or similar to PA/NH when f is small. The opposite effect can be observed when f is large. This is because, when f is large, more sensors are detected, including cluster-heads and normal sensors. In this case, it is better for the attacker to give priority to many normal sensors near it than giving priority to cluster-heads far from it. Giving priority to cluster-heads can initially decrease AC but the fall of AC is only temporary due to the cluster-head rotation (replacement of cluster-heads). Destroying more normal sensors reduces long term AC even if cluster-head rotations happen later to replace the destroyed cluster-heads. That is why when f is large, PA/NH makes the attack more effective.

The third observation we make from Fig. 2 (b) is, when f is extreme small, a large cluster size (C) results in less decrease of AC. When f is large, a larger cluster size reduces AC more significantly compared with a smaller cluster size. The reason is because, when f is extreme small, very few normal sensors or cluster-heads will be detected through active signals. In this case, a large cluster size means less number of clusters, which reduces the chance that a cluster-head is detected and destroyed. Consequently, AC is larger. However, when f is large, more number of cluster-heads will be detected irrespective of the cluster size. In this case, larger cluster size (C) increases the impact of destroyed cluster-heads on AC, thus decreases AC.

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 [1]. Some of the security concerns include resilient routing, secure communication, and electronic and physical node destructions. In [4], 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 [2] and the wormhole attack [3]. In [5], 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 [6], 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 [7] which provides two security protocols, SNEP and μTESLA. 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 [15], [1], [16], spoof, reply and message alter attack [4].

In [17], 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 [8], eavesdropping attacks, Sybil attacks etc. In [17] and [18], approaches to protecting the base station is 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 [8]. They also present design time factors that, if taken into consideration, reduces network vulnerability to DoS attacks. In [10], 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 [19]. 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 [19] is coverage and connectivity, while ours is the Accumulative coverage (AC)

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 [8]. Another class of

work like [20] 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 [21], [22], 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 attacks, the distribution of dead nodes are related to the motion of the search-based attacker. This changes the problem in that previously proposed purely fail-stop models are no longer applicable under the presence of a search-based physical 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 only compromised and hence are recoverable. In a prior work, we have identified and modeled blind physical attacks [9]. In [9], we studied the issue of deployment of sensors in a sensor network to meet lifetime requirement under blind attacks. Our focus in this paper is search-based physical attacks, which is quite different from blind attacks as mentioned in Section II.

VI. Conclusions

In this paper we addressed the issue of modeling search based physical attacks in sensor networks. Specifically, we first discussed the issue of signal classification from the attacker's perspective. We then identified critical features of search-based physical attacks and modeled a representative instance of search-based physical attacks. We studied performance impacts based on a novel metric that we defined, namely the Accumulative Coverage (AC). The accumulative coverage effectively captures both coverage and lifetime.

Our performance data clearly showed that search-based physical attacks dramatically reduces accumulative coverage (AC), further highlighting the importance of our work. We have made several important and interesting observations. First, larger attacker speeds, detection ranges and detection accuracy increases the effectiveness of attacks. Second, small active signal frequencies and large frequencies of cluster-head rotation can help maintain a large AC under attacks. Third, using a hierarchical sensor network has a mixed impact on maintaining AC under attacks; on one hand, the compromised cluster-heads (in hierarchical networks) cause decrease in AC significantly; on the other hand however, the existence of cluster-heads with cluster-head rotation can mislead the attacker and make its movements less efficient. Finally the impacts of the attacker and sensor network parameters interact with each other in affecting AC.

To the best of our knowledge, ours is the first work that identifies the problem and models search-based physical attacks. We however believe that this is just an important first step in this regard. There are other open issues in this subject. Our current ongoing work is focusing on modeling other variants of physical attacks. We are specifically focusing on modeling multiple physical attackers, co-operating among themselves. The orthogonal dimension of defending against physical attacks is also a part of our ongoing work.

References

[1] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," in *Communications of the ACM, Vol. 47, No. 6*, June 2004, pp. 53–75.

[2] J. R. Douceur, "The sybil attack," in *Proc. of 1st International Workshop on Peer-to-Peer Systems*, March 2002.

[3] Y. C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," in *Tech. Rep. TR01-384, Department of Computer Science, Rice University*, June 2002.

[4] 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*, May 2003.

[5] 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*, April 2004.

[6] Y. C. Hu, A. Perrig, and D. B. Johnson, "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.

[7] 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.

[8] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," in *IEEE Computer*, October 2002, pp. 54–62.

[9] 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.

[10] A. D. Wood, J. A. Stankovic, and S. H. Son, "Jam: A jammed-area mapping service for sensor networks," in *Communications of the ACM, Vol. 47, No. 6*, June 2004, pp. 53–75.

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

[12] N. B. Priyantha, A. Miu, H. Balakrishnan, and S. Teller, "The cricket compass for context-aware mobile applications," in *Proc. of Mobicom*, July 2001.

[13] D. Niculescu and B. Nath, "Ad hoc positioning system (aps) using aoa," in *Proc. of INFOCOM*, April 2003.

[14] J. Deng, R. Han, and S. Mishra, "Insens: Intrusion-tolerant routing in wireless sensor networks," in *University of Colorado, Department of Computer Science Technical Report CU-CS-9393-02*, 2002.

[15] 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 INFOCOM*, March 2004.

[16] 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.

[17] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *Proc. of the 2004 IEEE International Conference on Dependable Systems and Networks (DSN)*, June 2004.

[18] J. Deng, R. Han, and S. Mishra, "Enhancing base station security in wireless sensor networks," in *Technical Report CU-CS 951-03. Department of Computer Science. University of Colorado*, November 2002.

[19] S. Patil, "Performacne measurement of ad-hoc sensor networks under threat(s)," in *Proc. of IEEE Wireless and Communications and Networking Conference (WCNC)*, March 2004.

[20] R. J. Anderson and M. G. Kuhn, "Low cost attacks on tamper resistant devices," in *Proc. of the 5th International Workshop on Security Protocols*, April 1997.

[21] F. B. Schneider., "Implementing fault-tolerant services using the state machine approach: A tutorial," in *ACM Computing Surveys*, December 1990.

[22] 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.