Available online at www.sciencedirect.com
ScienceDirect
Computer Communications 30 (2007) 2546–2559
computer communications
www.elsevier.com/locate/comcom

Towards characterizing the effectiveness of random mobility against actuation attacks

Alexandra Czarlinska *, Deepa Kundur

Department of Electrical and Computer Engineering, Texas A&M University, 111D Zachry Engineering Center, College Station, TX 77843-3128, USA

Available online 21 June 2007

Abstract

Actuation functionality in a sensor network enables an unprecedented interaction with the physical environment. When used by a malicious distributed network however, actuation may become a potent new attack. In this work we explore a new general class of actuation attacks which aim to disable the sensing fidelity and dependability of a wireless sensor network. We propose a countermeasure to this Denial of Service on Sensing (DoSS) based on a controlled level of random mobility. We show how the level of mobility may be traded-off to suit security needs and energy constraints, and to exploit a priori knowledge of the environment. We demonstrate how this random mobility approach performs under various strengths, densities and distributions of the two networks and show that it reduces the number of affected nodes exponentially over time. Furthermore we discuss how this simple mobility approach renders the network more fault-tolerant and resilient in an inherent way without a need for the nodes to communicate and aggregate their sensed data.

Keywords: Security; Dependability; Actuation attack; Mobility; Sensing

1. Introduction

Wireless Sensor Networks equipped with actuation ability are quickly emerging as a topic of high interest. The ability of these networks to not only sense but also directly affect their surroundings allows an unprecedented bridge between the digital and physical worlds. This interaction with the environment widely increases the set of potential Sensor Actuator Network (SANET) applications and may render these networks more flexible and adaptable than traditional ones. Unfortunately it simultaneously opens the door to a new class of active and distributed attacks that cripple the sensing fidelity of networks through actuation.

We define actuation in sensor networks as the ability of a node to act upon, change or influence its environment using limited energy. The latter requirement is in contrast with robotic actuation where the robot typically has access to a much larger battery or wired source of energy. The small size (especially height) of the node and of its components further restricts the type and range of actuation that it may perform. The energy and size limitations imply that it might be advantageous for sensor nodes to distribute the actuation task throughout the network, thereby limiting the energy use of individual nodes while having a global effect on the environment.

Present research focuses largely on two types of actuation: mobility-based actuation and radio jamming attacks. In our work we wish to include these in the definition of actuation but broaden the class to include any actions which create an effect at the node's location which propagates outward from the node and possibly decays in strength with increasing distance. Examples of such actions include but are not limited to the dispersal of heat and of chemical agents through actuators such as diffusers or external fans. In such scenarios the actuation attack on the sensing fidelity of a legitimate sensor actuator network (lSAN) is carried out by a malicious sensor actuator network (mSAN) which is distributed throughout a common environment, with each malicious node performing its local

* Corresponding author.
E-mail addresses: czlinska@ece.tamu.edu (A. Czarlinska), deepa@ece.tamu.edu (D. Kundur).

0140-3664/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2007.05.030

actuation. Through this mSAN action, the legitimate network senses the deliberately actuated version of the phenomenon instead of phenomenon itself. This distributed actuation attack differs from other active attacks in that it does not attack the data *inside* the legitimate network, nor the routing and control data used to support the network. Rather the attack occurs at the physical or sensing level, affecting the environment being monitored before intelligence about it is collected. As such, current defense mechanisms against sensor network attacks are largely ineffective and the attack causes a Denial of Service on Sensing (DoSS) in the legitimate network. With its sensing fidelity compromised, the legitimate network reports false intelligence about the environment to the end user. This is particularly serious in applications where the lSAN is deployed for security and monitoring reasons, such as for biohazard and target detection.

The severity of the attack may be further understood by noting that due to its nature, it does not require the capture of any lSAN nodes or the breaking and use of its security keys. Furthermore its distributed form renders invalid the common assumption that only $k \ll N$ nodes in a network are attacked. Depending on the distributions with which the mSAN and lSAN deploy, the attacker could cover all or the majority of the lSAN nodes and affect them through actuation. This means that even a network deployed with high density and employing strategies such as majority voting or data correlation may fail to detect the attack. Dependable sensing (referred to as high sensing fidelity) must thus be achieved through other countermeasures.

In this paper we extend our work from [1] and propose the use of a controlled level of random mobility as an active type of actuation to counteract the DoSS. The approach is based on the philosophy that although we cannot use encryption to protect the integrity of the raw phenomenon as it travels from its source to the lSAN, that we may be able to use a form of steganography to "hide" part of the transmission channel from the attacker. Unlike more complex models of mobility and their accompanying protocols, the proposed random mobility requires limited computation and no communication among nodes. The level of mobility may also be augmented or decreased depending on the security needs and energy requirements. In the rest of the paper we show how this simple mobility model decreases the sensing error in the network exponentially in time, and how it is effective against various mSAN deployments, densities and actuation radii.

2. Related work

The use of actuation, whether as an attack or as a countermeasure mechanism, relates to and depends on various other fields of sensor network research. The following section provides a brief overview of some salient results (not intended to be fully comprehensive) from the areas of network security, coverage, localization, mobility and actuation as they pertain to the DoSS attack.

2.1. Sensor network security

Figs. 1 and 2 show the relationship of the actuation attack to other forms of active attacks found in the field of sensor network security. We observe that the actuation attack occurs before the phenomenon P under observation is sensed and recorded by the lSAN. This happens when the naturally noisy version of the phenomenon P, given by $\tilde{P}$, propagates through the environment and is actuated or altered by the mSAN to become an observable O. This possibly altered observable O is recorded by the lSAN as the true phenomenon and processed internally to produce some datum D. In contrast, other active attacks on sensor networks usually target data D flowing inside the network, or even the control and routing data. References [2] and [3] provide comprehensive discussions of recent attacks and countermeasures while reference [4] focuses specifically on Denial of Service (DoS) attacks in sensor networks. A critical factor in sensor network security is the issue of *physical* vulnerability of the nodes deployed in an unattended and possibly hostile environment which poses extra security challenges that have not been fully addressed to date [5,6,7]. The actuation attack is a type of DoS but it affects the network at this "physical" or sensing level which current countermeasures do not address. This is illustrated in Fig. 3 which shows traditional communication of data over a non-secure channel and in Fig. 4 which shows

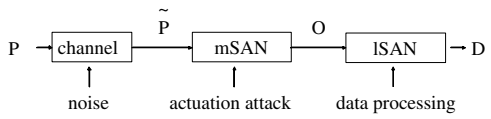

Fig. 1. Flow of information during an actuation attack.

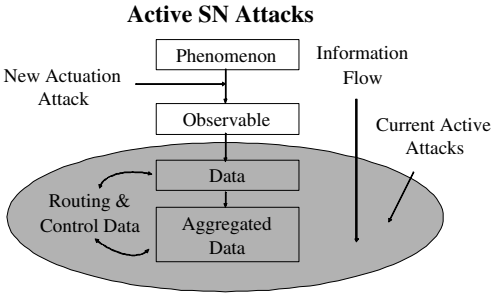

Fig. 2. Actuation vs. other attacks.

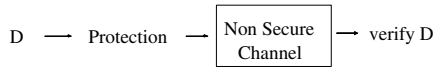

Fig. 3. Traditional communication over a non-secure channel.

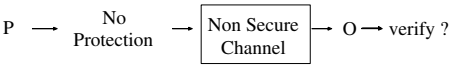

Fig. 4. Phenomenon communication over a hostile channel.

"communication" of a phenomenon over a non-secure channel. In the traditional case, if we wish to transmit a datum D over a non-secure channel we can rely on encryption. In the case of a sensor network deployed to monitor a phenomenon P, the phenomenon travels through a hostile channel before it is observed and recorded. Clearly no cryptographic protection of the raw phenomenon is possible before it arrives at the sensor network. We are thus forced to consider another approach to securing sensing fidelity in the face of actuation attacks in a hostile environment.

2.2. Coverage and location uncertainty

The exact definition of coverage varies depending on the specific application and on the toolsets used to address it. Generally speaking however, coverage is a measure of how well the sensor network covers or observes all the points of a physically distributed phenomenon. In [8,9,10] and [11] the authors formulate the Best and Worst case coverage scenarios by calculating a path of Maximum Support and Maximum Breach for an object moving through the sensor field. References [12,13,14, 15] and [16] present other key results in coverage. In reference [17] the authors use percolation theory to study the sensor network density required to achieve detection of a target with probability 1 almost surely. In [18] the authors consider the problem of coverage in the face of uncertainty in the sensor locations. In [19] the authors provide local algorithms for location discovery and coverage. This research is critical for understanding how an mSAN might find a path of least detection through the environment and how it might "cover" the lSAN nodes in the face of uncertainty of their locations.

2.3. Exposure and detection avoidance

In [20] the authors formulate exposure as a measure of how well an object moving on an arbitrary path can be observed by the sensor network over a period of time. The authors present an efficient algorithm for finding minimal exposure paths for the object to move along, which also simultaneously provides information about the worst case coverage of the sensor network. Simulation results show that for generally sparse fields with a random *uniform* spatial deployment, there exist many minimal exposure paths. The authors also present a generalized sensing model of interest to the study of actuation.

References [21] and [22] provide an approach that allows a stealthy traverse through an *unknown* environment that contains dynamic objects and an observer. The key is to exploit the dynamic objects in the environment as they become known and use their shadow as cover to move undetected from an initial location to a target location. The observer is assumed to have infinite observational range in all directions. The traversing robots are assumed to also have omni-directional sensing but for finite ranges. Simulations and implementation results show that 100% stealth can be achieved at a tradeoff of taking a route which is 86% efficient compared with a direct route which is 100% efficient but only 36% stealthy. These studies of exposure and detection avoidance are key to understanding how an intruding mSAN can deploy in an environment undetected.

2.4. Actuation

Mobility has been proposed as a flexible and effective tool for improving and extending a variety of network functions, from security to energy harvesting. In [23] the authors argue that controlled mobility (as opposed to merely opportunistic mobility) is able to enhance the sustainability of a sensor network, aiding with functions such as topology adaptivity, network capacity and fault isolation. In [24] the authors explore how mobility can be used by a sensor network as a type of actuation to repair its own coverage (called self-repair). In [25] the authors examine how mobile nodes can migrate to areas of high energy (solar for example) to charge themselves and then charge other starving nodes. In [26] the authors discuss how mobility can specifically help sensor network security by detecting misbehaving nodes. In [27] the authors introduce the idea of parasitic mobility where nodes are able to catch a ride on any moving object and dislodge from it using an actuator.

A number of pioneering works have proposed mobility as a type of active defense against the actuation attack of radio jamming. In [28] the authors study both the feasibility of launching jamming attacks and the challenges associated with detecting such attacks. Of particular interest is their observation that a single type of measurement usually does not suffice to correctly detect the attack. This correlates with our findings that without adequate side information (model of the attack or its parameters), detection is challenging and that involved protocols may not be most cost effective for the detection level they produce. In [29] the authors argue that mobility is advantageous to network operations and show how spatial escape strategies can prevent a mobile jammer from partitioning the network. Although similar in spirit to our work, the proposed mobility model requires some computation and further requires that the operational goals of the network be first expressed in terms of potential functions. Mobility of nodes ensues as a result of these potential forces and the associated network dynamics. Furthermore [29] focuses on attacking nodes that are concentrated in a specific region rather than distributed throughout the entire space as in our studies. In [30] the authors propose a mapping protocol which uses loose group semantics, eager eavesdropping, supremacy of local information and robustness to packet loss to detect jammed regions in real-time. This work once again focuses exclusively on jamming attacks – specifically on a subset of highly localized attacking nodes, and requires the use of a protocol to actively detect the attack.

These works suggest that including mobility to sensor networks significantly expands their functionality, autonomy and fault-tolerance. In Section 3 we extend our work from [1] and argue that mobility is a viable and effective countermeasure against attacks caused by other forms of actuation.

3. Problem formulation

This paper addresses DoSS attacks and countermeasures within the following framework. We consider a legitimate Sensor Actuator Network (lSAN) with N nodes deployed either deterministically or randomly throughout a finite physical region (which we call the "environment") to monitor a spatially distributed phenomenon of interest. A malicious Sensor Actuator Network (mSAN) is deployed either deterministically or randomly throughout the same environment with M nodes. We define the ratio of the number of mSAN nodes to the number of lSAN nodes as the flooding ratio $F.R$ where $F.R = M/N$. The spatial reach of an actuation attack emanating from an arbitrary mSAN node is given by the node's actuation radius $A.R$ which is assumed identical for each mSAN node. The larger the actuation radius, the further-reaching the attack. The region of actuation RoA centered at an mSAN node's location and corresponding to an actuation radius $A.R$ is given by $RoA = \pi\ (A.R)^2$. An lSAN node may find itself in the RoA of one or more mSAN nodes depending on the deployment of both networks.

Definition 1. Let $\gamma_n \geqslant 0$ be the number of lSAN nodes that are not influenced by the actuation attack at time n.

Definition 2. Let $\xi_n \geqslant 0$ be the number of influenced nodes at time n, where the influence may be caused by one or more mSAN nodes.

Definition 3. Let $A.F = \xi_n/N$ be the attack factor, measuring the ratio of the number of affected lSAN nodes to the total number of lSAN nodes N.

Definition 4. Let $\mathscr{C}$ be the total actuation coverage of the mSAN which is computed as the sum of the M RoAs minus any overlaps between the RoAs. Hence $\mathscr{C}$ in general depends on the specific realization of the mSAN deployment with $\mathscr{C} \leqslant M \cdot \pi(A.R)^2$.

From Definition 4 it is clear that in order to maximize the total area under its actuation influence, the mSAN should deploy such that its nodes are sufficiently apart and minimal overlap in the individual RoAs occurs.

3.1. Phenomenon and information flow

The lSAN is deployed in the environment to monitor a phenomenon of interest which can either be a point source phenomenon, such as a moving target, or a distributed phenomenon such as a temperature field. In our work we focus on spatially distributed phenomena which are slowly-varying for a sufficiently small time interval. In order to facilitate studies of actuation, we distinguish between three levels of information that exist between the phenomenon of interest and a sensor network as shown in Fig. 1. Let P denote the phenomenon of interest as it occurs in the environment. Let $\tilde{P}$ denote a possibly noisy version of P as it propagates through the environment from its source. Subsequently let O denote the observable that is sensed and recorded by a sensor node. When an actuation attack occurs O differs from $\tilde{P}$. Let D denote the data produced internally by a sensor node through the internal processing of O (such as averaging for instance).

3.2. Sensing model

We extend the general sensing model proposed in [20]. Eq. 1 presents the general sensing model S of a node i located at l_i monitoring a point p in the environment at time t and distance d away [20]. The parameters $\lambda_i(t)$ and $k_i(t)$ are technology-dependent and are generally allowed to vary with time due to errors and miscalibrations.

$$S_i(p,t) = \frac{\lambda_i(t)}{[d(l_i(t), p(t))]^{k_i(t)}} \tag{1}$$

We note that when $d = 0$ (node i is taking readings of $\tilde{P}$ at its own location l_i) this model produces infinite sensing. We propose a modified sensing model as shown in Eq. 2 that produces finite sensing at $d = 0$. This omni-directional model diminishes exponentially with distance and the sharpness of this decay can be controlled through the parameter γ to resemble Eq. 1 if desired. For simplicity we set $\lambda_i(t) = 1\ \forall\ i$ and $\forall\ t$, set $\gamma = 1$ and restrict the sensing range d as shown.

$$\begin{aligned} S_i(p,t) &= \lambda_i(t) \mathrm{e}^{-\gamma d(l_i(t), p(t))} \\ &= \begin{cases} \mathrm{e}^{-d(l_i(t), p(t))} & \text{if } 0 \leqslant d \leqslant d_{\max} \\ 0 & \text{if } d > d_{\max} \end{cases} \end{aligned} \tag{2}$$

3.3. Deployment and detection assumptions

For an actuation attack to proceed, the mSAN should be present in the environment without first being detected by the lSAN. To achieve this the mSAN might deploy in the hostile environment before the lSAN, or it might deploy alongside the lSAN before the latter establishes its infrastructure and begins monitoring. Furthermore as discussed in Section 2.3, work in detection avoidance provides certain algorithms for moving through a sensor network undetected. We must also consider the fact that most detection algorithms are designed for 2D environments and that the optimal placement of surveillance in the 3D case has been shown to be NP-complete [8]. For realistic surveillance applications the lSAN is deployed in a 3D environment where opponents can hide in valleys, behind bushes, employ camouflage and move around to create network

topology changes. We also note that mSAN nodes deployed by a reasonable attacker would most likely not be physically distinguishable from lSAN nodes (ie: visual surveillance through the use of camera sensors would not be sufficient) and that these nodes would most likely employ spreadspectrum techniques in their communications. Hence in most cases we cannot conclude that a hostile environment under the presence of an lSAN is free of the presence of a possibly actuating mSAN.

4. Actuation attack

We propose a simple model of an actuation attack where we abstract away the specific type of actuation and instead examine the actuation field produced. In proposing this model we wish to capture a salient feature common in many types of actuation (such as the actuation of heat or the release of chemical agents). In many of these phenomena, the original concentration is centered at or near the actuating node. It then dissipates or propagates outward, where it possibly decays in strength with increasing distance from the node. As such, we model an actuation by an arbitrary mSAN node j as centered at the node's location l_j and (possibly) decaying away in all directions from the node.

In general a node j may be able to produce around it an actuation field $a_j(x,y,t)$ which may or may not be symmetrical w.r.t x and y nor constant with t. In this work we consider the simplest case where $a_j(x,y,t) = 1$ for $\forall\ t$ and $\forall\ j$, that is, each node produces a constant field of arbitrary magnitude of 1. The actuation begins at some time t_0 at which point it is only present at node j's location denoted by l_j. The spatial propagation of the phenomenon is modeled by a decaying exponential given by Eq. 3.

$$\begin{aligned} A_j(p,t) =& a_j(x,y,t)\cdot \mathrm{e}^{-d(p,l_j(t))} \\ =& 1\cdot \mathrm{e}^{-d(p,l_j)}, \\ & t_0 \leqslant t \leqslant t_F, 0 \leqslant d \leqslant d_{\max} \end{aligned} \tag{3}$$

$A_j(p,t)$ denotes the actuation effect of node j at spatial point $p(x,y)$ at time t. The spatial point p can be for instance the location of an lSAN node and is in general allowed to be time-varying (mobile lSAN nodes) while for simplicity we assume that the mSAN nodes are stationary that is, $l_j(t) = l_j\ \forall t, \forall j$. We note that the actuation effect is negligible outside of the specified distance and time range. In conclusion we assume that the only actuation performed by the lSAN is mobility while the only actuation performed by the mSAN is phenomenon actuation as described by Eq. 3. Furthermore we assume that the mSAN nodes do not dynamically coordinate with each other during the actuation but rather are programmed to start and continue actuating for a specified time. We also assume that in general the lSAN does not have an internal model of the actuation or its parameters but may or may not have a limited a priori model of the phenomenon P.

A point p in the environment contains the possibly noisy version of the phenomenon $\tilde{P}$ (due to natural propagation, not due to actuation) and it might come under the actuation influence of several mSAN nodes. Hence the strength of the sensed Field at any point p and time t obtained through this superposition is given by Eq. 4:

$$F(p,t) = \Sigma_{j\in M} A_j(p,t) + \tilde{P}(p,t) \tag{4}$$

Specifically if the point p is the location of a mobile lSAN node i and if the actuation attack is as given in Eq. 3 then:

$$\begin{aligned} F(i,t) =& \Sigma_{j\in M} A_j(l_i,t) + \tilde{P}(l_i,t) \\ =& \Sigma_{j\in M} 1\cdot \mathrm{e}^{-d(l_i,l_j)} + \tilde{P}(l_i,t) \end{aligned} \tag{5}$$

where the distance d and the time t are constrained as stated earlier. Given a random spatial deployment of the mSAN nodes, $F(p,t)$ will vary throughout the environment with p and t.

4.1. Energy considerations

Among the various resource constraints in WSNs, the energy constraint is considered one of the most significant and restrictive. It is of particular importance in the case of actuation, where malicious nodes use their energy not only to sense but also to act upon the environment. The feasibility of such an attack based on energy constraints must be considered.

We argue that energy constraints do not prevent an actuation attack from happening for several reasons. (1) While a legitimate WSN is expected to minimize its energy expenditure to ensure longevity of operation, the goal of the malicious network may be a direct short-lived attack after which the mSAN will stop operating. In this context the mSAN can afford to expand its energy in a collective effort to cause a DoSS in the lSAN. (2) The attack is distributed and hence each attacking node needs to contribute only a fraction of the overall required energy. (3) Research in sensor network energy suggests that nodes may harvest or replenish their energy from the environment [25]. (4) Certain types of actuation may require relatively little energy, such as transmitter and sensor jamming through noise generation. Furthermore, the amount of energy required by each node is proportional to the duration of actuation Δt and on the change in the phenomenon ΔP desired. For small ΔP and Δt, the amount of required energy may be small.

5. Mobility-based countermeasures

We seek a countermeasure to the actuation attack which satisfies the following criteria as closely as possible.

(i) Allows all or the majority of the lSAN nodes in an area to recover their sensing fidelity given that little side-information may be known about the attack or its parameters.

(ii) Minimizes the amount of required node communication and higher-level data aggregation, in essence allowing nodes to fault-repair as autonomously and locally as possible.
(iii) Controls energy expenditure and allows for a trade-off between security and energy costs.
(iv) Controls changes in network topology to limit additional burdens on routing and control of the network.

We propose that the countermeasure be partly evaluated based on the following metrics: the Average Sensing Error (E) given by Eq. 6, the Percent Improvement in Average Sensing Fidelity (PI) given by Eq. 7 and the Percent lSAN nodes affected (PA) given by Eq. 8, where $A.F$ is the attack factor from definition 3.

$$E(t) = \frac{1}{N}\Sigma_{i\in N}E_i(t) \tag{6}$$

$$PI = \frac{E(t_0) - E(t_f)}{E(t_0)} \cdot 100\% \tag{7}$$

$$PA(t) = A.F \cdot 100\% \tag{8}$$

Based on these requirements, we propose the following tactic or design philosophy. As shown in Figs. 5 and 6 we argue that the above criteria can be met if we find a way to provide *some* copies of $\tilde{P}$ to the lSAN, given that an actuation is occurring and that the observable O is generally not the same as $\tilde{P}$ (in Fig. 6, "Worst Case Actuation Attack" refers to the scenario where the mSAN is able to affect all or the majority of the lSAN nodes). Since the lSAN receives both copies of $\tilde{P}$ and of O, ideally we want the countermeasure to provide $k \geqslant N/2$ copies of $\tilde{P}$.

Given that any spatial deployment (either deterministic or stochastic) of the lSAN and mSAN nodes is allowed, any number k of lSAN nodes may be affected by the actuation, where $k < N$ but possibly as large as $k \sim N$. This is particularly detrimental in the special case where the mSAN has a good estimate of the locations of the lSAN nodes. Some of the most damaging active attacks on WSNs in current literature assume that the attacker is able to capture a number of nodes and obtain their cryptographic keys. In the case of an actuation attack the distributed attacker does not capture nodes or their keys. The success of the attack depends largely on the mSAN's ability to distribute itself correctly around the lSAN nodes undetected. In this context the *location* of the lSAN nodes becomes the "secret key" which we wish to hide or at least render unpredictable for the attacker. Hence we conclude that the significance of node location information in securing the dependability of WSNs is large. This observation implies that if we can render the position of the lSAN unpredictable to the attacker, that we may prevent the mSAN from obtaining an optimal spatial distribution with which to carry out the attack. This can be achieved through random mobility of the lSAN nodes. In essence, although we are clearly not able to *encrypt* the raw phenomenon at the source before it is altered, we may be able to use mobility to *hide* part of the "communication channel" from $\tilde{P}$ to the lSAN nodes – this is conceptually akin to using steganography instead of cryptography. Hence we argue that given limited side information, mobility-based approaches (where mobility is a form of actuation), hold significant potential for dependability against actuation attacks.

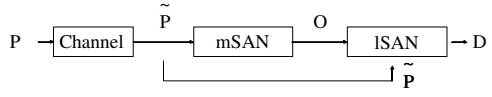

Fig. 5. To mitigate an actuation attack the lSAN needs access to $\tilde{P}$.

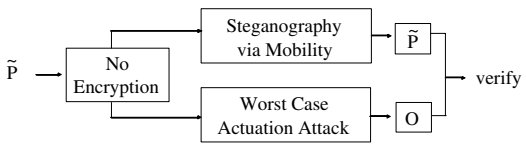

Fig. 6. Use of mobility to hide part of the channel (akin to steganography).

5.1. Mobility model

Given our model of P as slowly-varying over time for sufficiently small ΔT and given the design philosophy, we propose a mobility model that meets the countermeasure requirements. In [31] the authors describe a variety of node mobility models for possible use in ad hoc networks. Among these models the simplest 2D version is arguably the Random Walk Mobility Model, where the movement of each node is controlled by a random speed in the range $[speed_{\min}, speed_{\max}]$ and a random angle or direction of movement in the range $[0, 2\pi]$. Once a new speed and direction are selected, a node travels according to these directions for either a set distance or a set amount of time. No extra computation or coordination among the nodes is required, as each node makes decision independently. Another key feature of this model is that each node experiences a type of Brownian motion, generally roaming around a location (the roaming area depends on d) without completely leaving the area and thus changing the network topology [31].

As later shown with analysis and simulations, we argue that this simple mobility model is generally sufficient to disrupt a distributed actuation attack, given that this attack depends heavily on the relative position of the mSAN nodes w.r.t the lSAN nodes. We wish to augment this mobility model such that it allows us to trade-off security against energy use. This is accomplished through the introduction of a mobility threshold $M.T \geqslant 0$. The $M.T$ of a node is the minimum change in the observable from a previous measurement required for a node to move. In other words, node i moves randomly according to the Random Walk mobility model if $\Delta O_i(\tau) = |O_i(t_k) - O_i(t_{k+\tau})| > M.T_i$ where τ is the sampling interval, $O_i(t)$ is an observable collected by node i

at time t and $M.T_i$ is the mobility threshold of node i. For instance, if we set $M.T = 0.3$ then node i will only move if it records a 0.3 change in the observable from the previous time instance.

The mobility threshold of the nodes can be based on security requirements as follows. If we require a high sensing fidelity, we may set $M.T$ to a small value closer to 0. This means that a node will verify its sensed observable (by moving to a new location), as soon as it detects a small change occurring in the environment under observation. A trade-off between security and energy consumption can be achieved by setting $M.T$ to a larger value. On the other hand, we may wish to exploit any a priori information about the phenomenon under observation when setting the mobility threshold. In many cases it is not feasible to obtain the probability density function of a phenomenon. However if we possess side-information about the autocorrelation of the phenomenon, we may wish to use it to set the $M.T$. For instance, we might expect that a naturally occurring P might vary with $\Delta\ O(\tau) < 0.3$ and hence set $M.T = 0.3$. The selection of such thresholds for various phenomena is a subject of ongoing study, along with studies of how aggregator nodes and base stations may be used to control the probability of false alarm due to oversensitive or poorly selected thresholds.

6. Analysis

We wish to analyze the effectiveness of random mobility in reducing the attack factor $A.F$ and hence in repairing the sensing fidelity. We require a definition of the number of affected and unaffected nodes as given by Definitions 1 and 2, and we also need to capture the change in the status of a node (affected or unaffected) due to mobility.

Definition 5. Let $\bar{p} \geqslant 0$ denote the probability that an lSAN node is in the region of actuation (RoA) of one or more mSAN nodes, and that it stays in this region in the next time instant.

Definition 6. Let $\bar{q} \geqslant 0$ denote the probability that an lSAN node is not in the *RoA* but moves into it in the next time instant.

For simplicity we assume that each lSAN node is deployed according to a uniform distribution in the $2D$ space. According to our mobility model, each node effectively travels a random distance d (based on velocity and time of travel) and a random direction in the range of $[0, 2\pi]$. Though d is usually locally restricted, for the purposes of analysis we do not place this restriction, allowing a node to move to any location in the $2D$ space. Hence we obtain the following result regarding the probability $\bar{p}$ that a lSAN node stays in the *RoA* of one or more mSAN nodes.

Lemma 1. *For a 2D environment with dimensions d_x by d_y and M actuating nodes, $\bar{p} \leqslant \frac{M\cdot\pi(A.R)^2}{d_x d_y}$.*

Proof 1. Let Y_l be the *lth* lSAN node where $l = 1,2,\ldots,N$ and let $\mathbf{m} = [m_1, m_2, \ldots, m_M]$ be the set of the mSAN nodes. Then $\bar{p} = P[Y_l \in RoA(\mathbf{m})] = \frac{\mathscr{C}}{d_x \cdot d_y}$ where $\mathscr{C}$ is the total actuation coverage of the mSAN. Since $\mathscr{C} \leqslant M \cdot \pi(A.R)^2$ by the union bound, $\bar{p} \leqslant \frac{M\cdot\pi(A.R)^2}{d_x d_y}$. □

Note 1. In general $A.R$ is small compared with the dimensions of the world d_x, d_y. Hence $\bar{p} \leqslant \frac{M\cdot\pi(A.R)^2}{d_x d_y} \leqslant 1$.

To understand how the number of affected and unaffected lSAN nodes changes with mobility over time, we note that the relationship can be represented succinctly with the markov relation shown in Fig. 7 where γ_n is the number of unaffected nodes at time n, ξ_n is the number of affected nodes and where $\gamma_n + \xi_n = N$ for any given time n. The probabilities of transition at each time step are given by $\bar{p}$ and $\bar{q}$. We note that the probability $\bar{q}$ that a node is not in a *RoA* and moves into such a region in the next time instant is related to a mobility threshold $M.T$ that was picked incorrectly (made too sensitive for the given phenomenon for instance). For simplicity we assume that $\bar{q} \approx 0$. Hence we obtain the following result regarding the average number of unaffected nodes at any time instant n.

Theorem 1. *Let N be the total number of lSAN nodes, let $\bar{p}$ be the probability that an lSAN node is in the RoA of one or more mSAN nodes and assume that $\bar{q} = 0$. Then the average number of lSAN nodes not influenced by actuation at time n is given by $E[\gamma_n] = N(1 - \bar{p}^{n+1})$.*

Proof 2. From the binomial distribution with $\bar{q} = 0$ we note that $E[\gamma_0] = N(1-\bar{p})$ and $E[\xi_0] = N - E[\gamma_0] = N\bar{p}$ where $\gamma_n + \xi_n = N$. From Fig. 7, $E[\gamma_n] = E[\gamma_{n-1}] + E[\xi_{n-1}](1-\bar{p}) = E[\gamma_{n-1}] + (N - E[\gamma_{n-1}])(1-\bar{p}) = \bar{p}E[\gamma_{n-1}] + N(1-\bar{p})$. Hence solving the recursion equation for $E[\gamma_n]$ we obtain the result. □

With this result in hand we are now able to characterize the effect of mobility on the attack factor $A.F$.

Theorem 2. *The expected value of the attack factor is given by $E[A.F] = E[\xi_n]/N$. Given a strategy of random mobility, $E[\xi_n]/N \to 0$ as $n \to \infty$. Furthermore, $\xi_n/N \to 0$ as $n \to \infty$.*

Proof 3. $E[A.F] = E[\xi_n]/N = (N\text{-}E[\gamma_n])/N$, since $\gamma_n + \xi_n = N$. Therefore $E[A.F] = 1 - (1 - \bar{p}^{n+1})$ from Theorem 1. Therefore $E[A.F] = \bar{p}^{n+1}$. In the limit as $n \to \infty$, $\bar{p}^{n+1} \to 0$. Furthermore since $A.F \geqslant 0$, therefore $A.F \to 0$ as $n \to \infty$. □

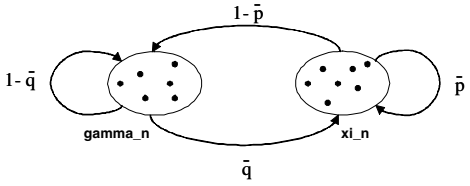

Fig. 7. Relationship between the number of affected and unaffected nodes at any time n.

Theorem 2 states that the attack factor $A.F$ decreases exponentially with increasing time n and that it approaches 0 for large n. In the next section we present simulation results to confirm this analysis and to explore other aspects of the random mobility approach.

7. Experimental results and insights

In this section we present simulation results to study the characteristics of controlled random mobility in mitigating actuation attacks. Specifically we examine the decrease in the $A.F$ or number of affected nodes, and the corresponding reduction in the sensing error. This is carried out for various flooding ratios, actuation radii, mobility thresholds and deployment distributions. We focus on the Gaussian and Uniform distributions with the former chosen to represent the family of related exponential distributions (Laplace, Exponential etc.) and with the latter as a distribution not fitting this family.

The simulations were performed using a Matlab-based simulator that was developed. In the simulations the travel distance of the lSAN nodes was on average 3 spatial units/time interval while the angle ranged uniformly from $[0, 2\pi]$. The simulation time interval was set to 300 time units. The sensing range of each lSAN node was taken as 3 spatial units while the actuation range $A.R$ of the mSAN was varied from 1 to 3 spatial units. To generate a (x, y) coordinate according to a uniform distribution, the x and y coordinates were each chosen from a uniform distribution. This method was also used for the Gaussian distributions. The size of the simulation world was set to 50×50 U^2. The number of lSAN nodes was held constant at 300 while the number of mSAN nodes was varied from 1 to 600 to obtain various flooding ratios $F.R$. Without loss of generality the phenomenon P was set to 0 in Eq. 5 and hence any actuation by the mSAN recorded by the lSAN as an observable constituted an error. The Average Sensing Error of the lSAN was computed using Eq. 6. The lSAN sensing was implemented using Eq. 2, the actuation was implemented using Eq. 3 and the superposition from actuating nodes was obtained using Eq. 5. The figures of merit to evaluate the success of the DoSS countermeasures were: 1: Average Sensing Error E given by Eq. 6, 2: Percent Improvement in Average Sensing Fidelity PI given by Eq. 7 and 3: Percent lSAN nodes affected given by Eq. 8.

7.1. Effect of controlled random mobility

We begin with a look at the impact of actuation on a legitimate sensor network. Fig. 8a shows an lSAN (small circles) and an mSAN (diamonds) deployed concurrently according to uniform distributions. Large open circles denote the actuation radii of the mSAN nodes, and small filled circles represent lSAN nodes that have been affected by the attack. Fig. 8b shows the reduction in the $A.F$ after controlled random mobility is used by the lSAN and Fig. 9a shows the average sensing error as it is reduced over time through mobility in a seemingly exponential decay. Fig. 9b shows this reduction in sensing error for various flooding ratios where $F.R = M/N$ and where $F.R = 1$ is the weakest attack. We note that the strategy reduces the sensing error even when there are on average 3 enemy nodes for each lSAN node ($F.R = 3$).

7.2. Effect of deployment distributions

Next we would like to examine how different deployments affect the severity of an actuation attack (given that the analysis focused on Uniform deployments) and test if mobility helps regardless of the deployment used. Fig. 8a shows a typical uniform deployment of both networks with 300 lSAN nodes (circles) and 300 mSAN nodes (diamonds) giving a flooding ratio $F.R = 1$. For comparison Fig. 10a shows a grid distribution for both networks and the corresponding actuation effects. Fig. 10b depicts a typical Gaussian deployment for both networks where the lSAN

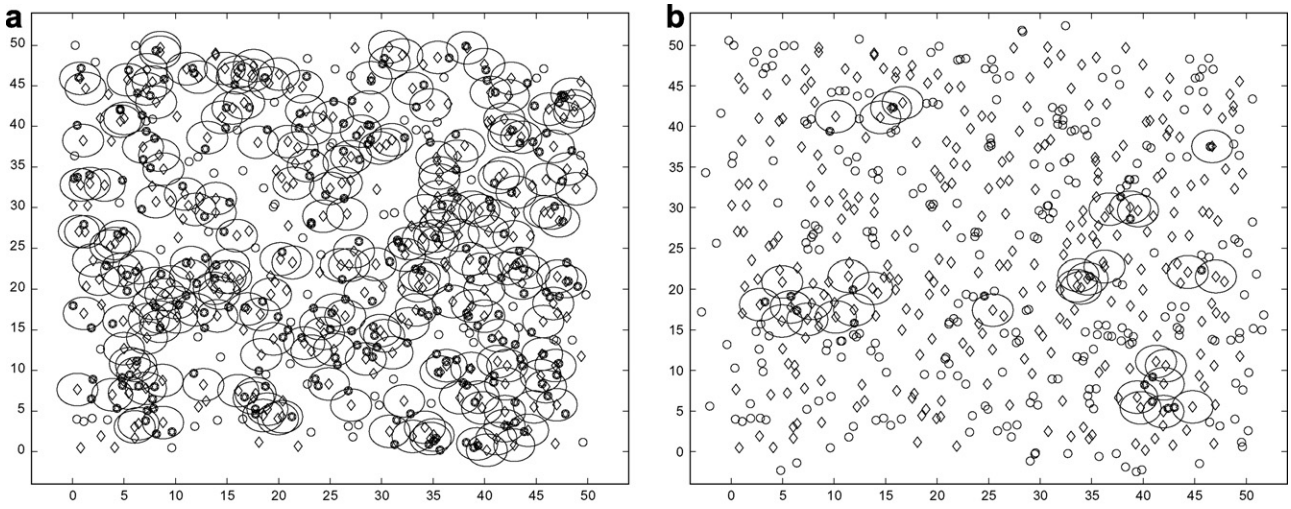

Fig. 8. (a) Attack before mobility. (b) After mobility.

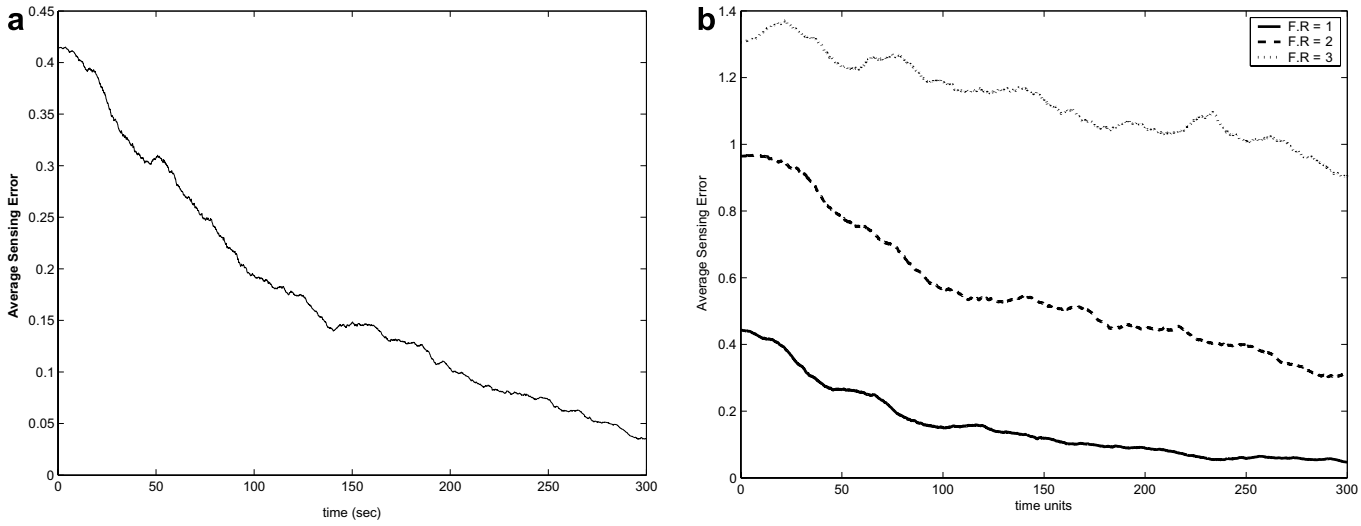

Fig. 9. (a) Reduction in average sensing error. (b) Efficacy under various *F.R*s.

is deployed with arbitrary mean $\mu_x = 25$, $\mu_y = 40$ and variance $\sigma_x^2 = 20$, $\sigma_y^2 = 20$. The mSAN is also deployed with a Gaussian distribution but given by $\mu_x = 40$, $\mu_y = 40$ and $\sigma_x^2 = 20$, $\sigma_y^2 = 20$ with $A.R = 2$. From these three representative deployments we note the large number of affected lSAN nodes when no countermeasures are in place, with the most severe effect occurring for a deterministic grid deployment (all nodes may be affected).

In a worst case attack the mSAN can estimate the distribution with which the lSAN is deployed (though the exact parameters may not be known as in the Gaussian example given above) and deploy with the same distribution. Figs. 11a and b show the resulting percent ($\times 10^{-2}$) nodes that are affected by the attack and the resulting average initial sensing error (before any countermeasures) for various flooding ratios. These results are shown for the case when 1-both networks deploy using a Uniform distribution, 2-both networks deploy using a Gaussian distribution and the mSAN has a good estimate of the lSAN distribution parameters and 3-where both deploy using a Gaussian distribution but the mSAN has a poor estimate. For cases 2 and 3 the lSAN was assigned the parameters mentioned earlier. The mSAN distribution for case 2 was set as $\mu_x = 23$, $\mu_y = 38$ with $\sigma_x^2 = 20$, $\sigma_y^2 = 20$. For case 3 it was set as $\mu_x = 15$, $\mu_y = 15$ with $\sigma_x^2 = 20$, $\sigma_y^2 = 20$. Fig. 12a shows a typical reduction in the sensing error when mobility with $M.T_i = M.T = 0\ \forall i$. We see that the average final sensing error is decreased dramatically due to mobility and reduced by 100% in the Uniform case even when the flooding ratio is as high as 2. We also note that when the two networks are deployed according to a Gaussian distribution and when the mSAN knows the parameters well, that the attack is most severe (second only to a grid deployment). Fig. 12b shows the decrease in sensing error over time for the Gaussian Case 2 with $A.R = 2$ and various mobility sets. Mobility set $MT1$ causes all nodes to move

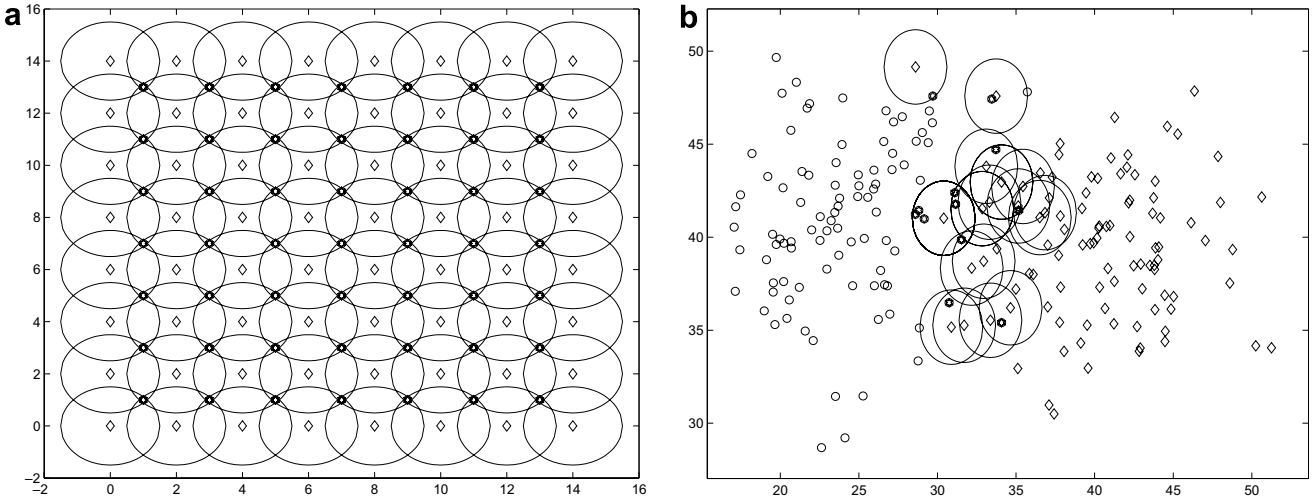

Fig. 10. (a) 64 mSAN nodes vs. 49 lSAN nodes with a grid pattern. (b) 100 mSAN nodes vs. 100 lSAN nodes with a Gaussian deployment.

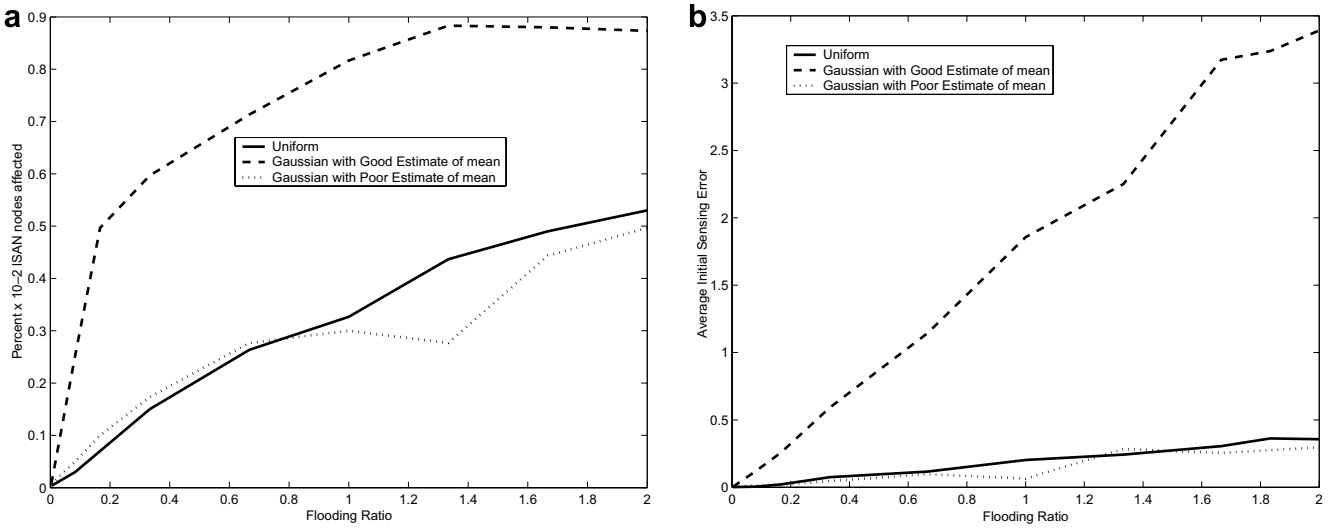

Fig. 11. (a) Initial Percent $\times 10^{-2}$ of affected nodes for various distributions and $AR = 1$. (b) Average Initial Sensing Error for Various Distributions with $AR = 1$.

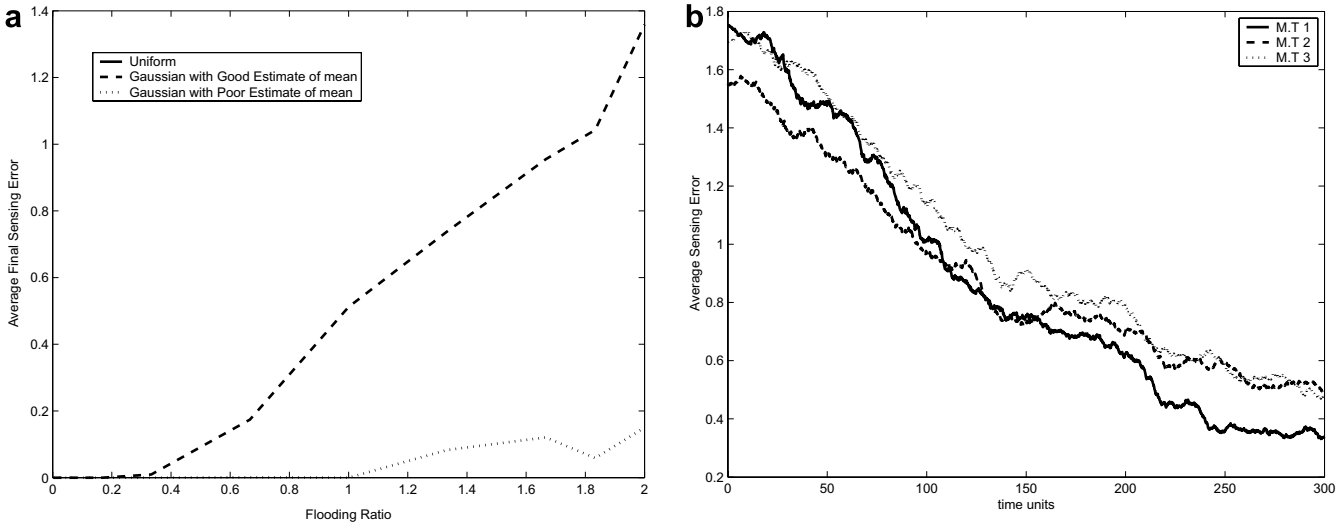

Fig. 12. (a) Average Final Sensing Error for Various Distributions with $AR = 1$. (b) Reduction in sensing error over time for the Gaussian with a good estimate with $F.R = 2$ and $A.R = 2$ and various mobility sets.

with mobility threshold $M.T = 0$. Mobility set $MT2$ causes 25% of the nodes to move with threshold $M.T = 0$, 25% to move with $M.T = 0.3$, 25% to move with $M.T = 0.6$ and 25% to move with $M.T = 1$. Mobility set $MT3$ causes 50% of the nodes to move with threshold $M.T = 0$, 25% to move with $M.T = 0.3$, 13% to move with $M.T = 0.6$ and 12% to move with $M.T = 1$.

7.3. Effect of actuation radii

We would like to explore the effect of various actuation radii, where the larger the actuation radius of each node, the more spatially powerful the attack. Fig. 13 shows the percent ($\times 10^{-2}$) of lSAN nodes affected for $A.R = 1$, $A.R = 2$ and $A.R = 3$ when deployed in a Uniform distribution. Fig. 14a shows the corresponding average initial error in sensing fidelity before mobility and Fig. 14b shows the average final sensing error using mobility of $M.T = 0$. We conclude that in the case of $A.R = 1$, mobility reduces the average sensing error by as much as 100%. For a stronger attack of $A.R = 3$, the reduction is on the order of 20% for this choice of MT. We observe that the sensing error increases in a seemingly linear way with increasing flooding ratio regardless of the $A.R$ used. Mobility on the other hand appears to reduce the sensing error in a nonlinear way with respect to flooding ratio. Importantly, in the case of $A.R = 2$ (there are 2 malicious nodes for every legitimate node), mobility still improves the sensing fidelity for all flooding ratios.

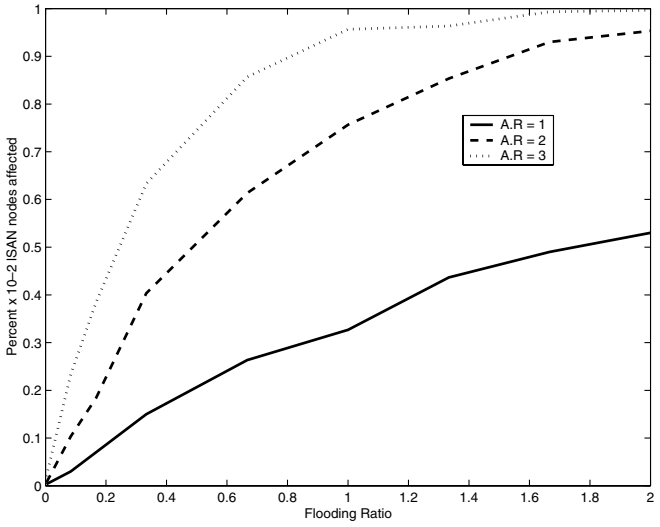

Fig. 13. Percent $\times 10^{-2}$ initially affected nodes (before mobility) for a uniform distribution for various radii of actuation.

7.4. Effect of mobility threshold

Next we examine the trade-off between reducing the sensing error and the level of lSAN mobility required as controlled by the mobility threshold $M.T$. A lower $M.T$ indicates higher mobility and we note that for $M.T_i = M.T\ \forall i$, the smaller the $M.T$, the larger the percent of nodes that move at any time instant. Fig. 15a shows the improvement in sensing when $M.T = 0.3$ is used for *all* nodes with a Uniform distribution for various actuation radii, and Fig. 15b shows these results for $M.T = 1$ for all nodes. We conclude that although in general a $M.T = 0$ provides best results (reducing the sensing error to 0% in the case of $A.R = 1$ for instance), that such a high mobility is not always required to reduce the sensing error. Importantly we note that the mobility threshold $M.T = 0$ was included in the simulations to test the effectiveness of such an extreme setting. In most practical scenarios this threshold would be increased from 0 to account for internal sensor errors.

Tables 1–3 show the trade-off between the *maximum* percent of nodes that move during any time instant within the simulation interval $t_0 \leqslant t \leqslant t_f$, and the average percent of nodes still affected by actuation at time t_f. Table 1 corresponds to $F.R = 1/3$, Table 2 to $F.R = 1$ and Table 3 to $F.R = 2$. Each entry (A, B) in a table corresponds to (% nodes affected after mobility, % max nodes move). Cells shaded in grey indicate cases where the countermeasure goal was fully achieved with a majority of lSAN nodes completely free of mSAN actuation. For the remaining cases we note two critical points: 1 – although most nodes remain affected, at least one clean copy of $\tilde{P}$ exists (in most cases dozens of copies exist). Hence the lSAN has at least one record of what really occurred in the environment at a particular instant. 2 – Although most nodes are still affected at the end of the time interval, most have *reduced* their sensing error by moving to a less affected area. The tables count *all* affected nodes even if the sensing error at those nodes is small.

It is also interesting to test the effect of mobility when all the lSAN nodes are *not* set to the same mobility threshold. To this end we created three mobility sets as described in Section 7.3. Mobility set 1 has all nodes moving with $M.T = 0$, mobility set 2 has 25% of the nodes moving with $M.T = 0$, 25% with $M.T = 0.3$, 25% with $M.T = 0.6$ and 25% with $M.T = 1$, while mobility set 3 has 50% moving with $M.T = 0$, 25% with $M.T = 0.3$, 13% with $M.T = 0.6$ and 12% with $M.T = 1$. Mobility thresholds were assigned randomly to each node such that the overall statistics matched the parameters of a given mobility set. Fig. 16a shows the reduction in sensing error over time for $A.R = 1$

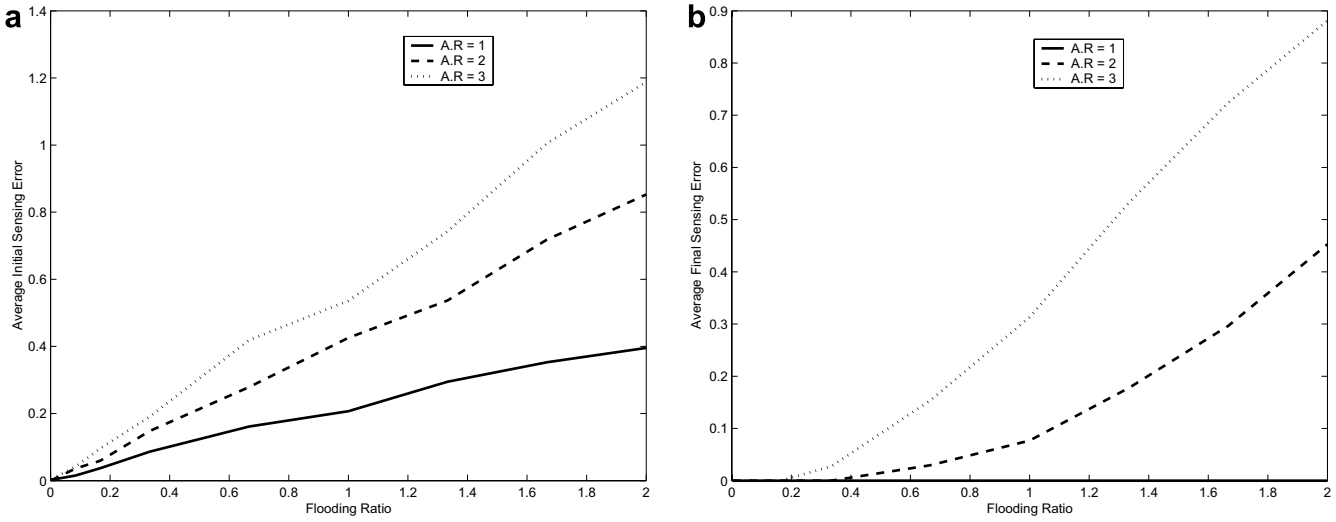

Fig. 14. (a) Average initial sensing error for a uniform distribution and various $A.R$ (b) Average final sensing error after mobility with $M.T = 0$.

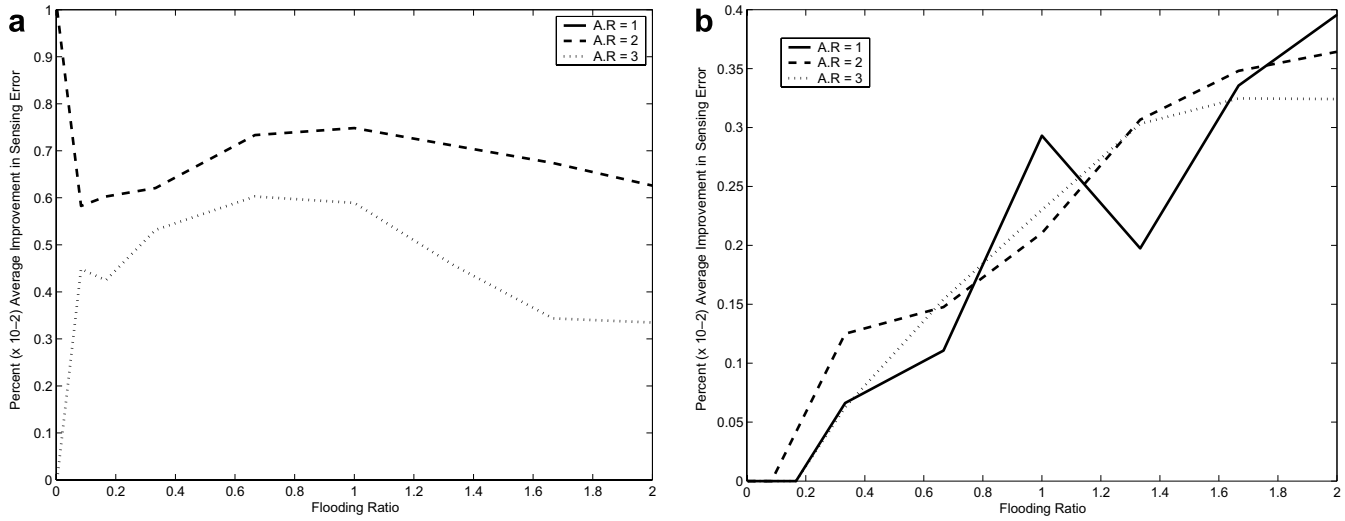

Fig. 15. (a) Percent $\times 10^{-2}$ Improvement in Sensing after Mobility for a Uniform Distribution for various Actuation Radii and $M.T = 0.3$. (b) $M.T = 1$.

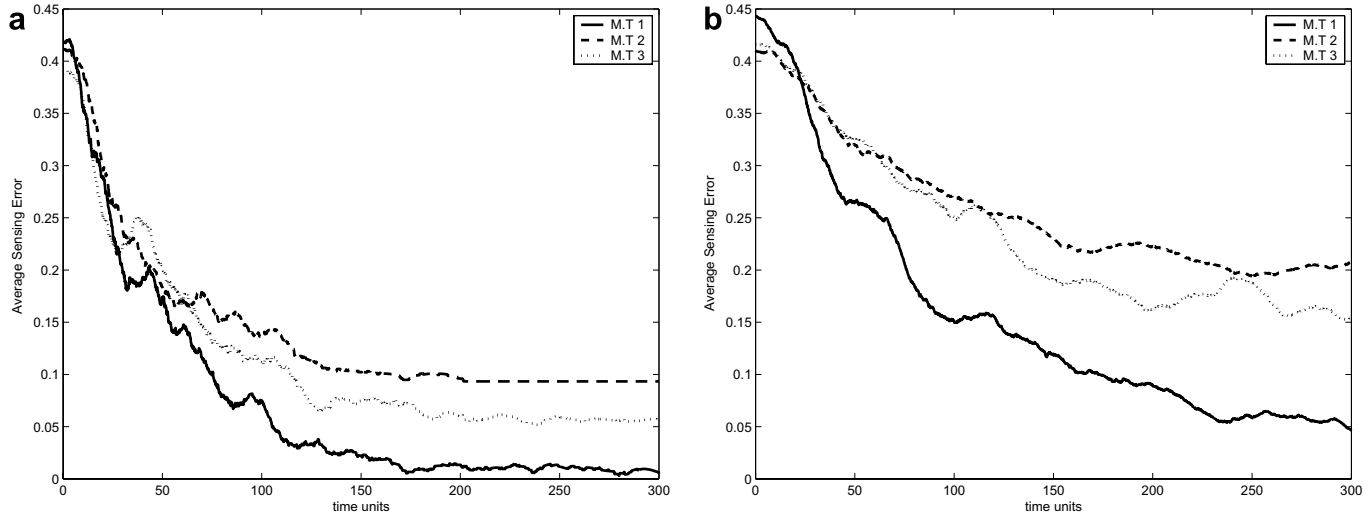

Fig. 16. (a) Uniform distribution $A.R = 1$, $F.R = 2$ for the three mobility sets. (b) Uniform distribution $A.R = 2$, $F.R = 1$ for the three mobility sets.

Table 1
$F.R = 1/3$

	M.T = 0	M.T = 0.3	M.T = 0.6	M.T = 1
A.R = 1	(0.01, 43.1)	(17.9, 16.9)	(34.0, 1.10)	(36.8, 0.20)
A.R = 2	(0.00, 12.6)	(0.02, 13.1)	(11.5, 0.19)	(12.9, 0.28)
A.R = 3	(8.99, 66.2)	(61.2, 22.9)	(63.0, 8.10)	(62.1, 1.32)

Table 2
$F.R = 1$

	M.T = 0	M.T = 0.3	M.T = 0.6	M.T = 1
A.R = 1	(0.00, 33.1)	(0.00, 24.2)	(22.3, 0.86)	(26.4, 0.21)
A.R = 2	(6.30, 77.8)	(45.2, 51.2)	(63.2, 24.2)	(71.3, 0.79)
A.R = 3	(55.0, 96.0)	(81.5, 43.7)	(91.2, 23.8)	(92.0, 10.3)

and $F.R = 2$ for the three mobility sets, while Fig. 16b shows the results for $A.R = 2$, $F.R = 1$. We note that sets where only *certain* nodes have low mobility thresholds

Table 3
$F.R = 2$

	M.T = 0	M.T = 0.3	M.T = 0.6	M.T = 1
A.R = 1	(0.00, 50.1)	(0.01, 50.2)	(34.9, 26.1)	(51.4, 0.76)
A.R = 2	(38.2, 93.2)	(68.7, 70.9)	(83.6, 53.0)	(90.4, 28.0)
A.R = 3	(74.9, 100)	(94.0, 91.6)	(95.5, 71.5)	(99.0, 41.0)

(hence higher verification ability) still perform relatively well.

8. Conclusions

Based on a proposed model of an actuation attack, we study the resulting loss in sensing fidelity (or sensing error) for a number of different deployments, actuation radii and flooding ratios. We study controlled levels of random mobility as a countermeasure for this attack

using various mobility thresholds to trade-off between sensing fidelity, security, energy and a priori knowledge of the phenomenon. We show through analysis and simulation that controlled random mobility decreases the number of affected nodes exponentially over time. We also demonstrate that not all nodes must be set to a high mobility level in order to reduce the sensing error, and that effective mobility sets may be constructed instead. We conclude that mobility reduces the average sensing error of the lSAN under a variety of conditions, even under heavy mSAN node flooding and large actuation radii.

References

[1] A. Czarlinska, D. Kundur, Distributed actuation attacks in wireless sensor networks: implications and countermeasures, in: 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 3–12.

[2] L. Buttyan, J.-P. Hubaux, Report on a working session on security in wireless ad hoc networks, Mobile Computing and Communications Review 6 (4) (2002) 1–17.

[3] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Next century challenges: scalable coordination in sensor networks, in: Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking, 1999, pp. 263–270.

[4] A.D. Wood, J.A. Stankovic, Denial of service in sensor networks, IEEE Computer 35 (10) (2002) 54–62.

[5] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Communications of the ACM 47 (6) (2004) 53–57.

[6] H. Chan, A. Perrig, Security and privacy in sensor networks, IEEE Computer 36 (10) (2003) 103–105.

[7] D. Wagner, Resilient aggregation in sensor networks, in: SASN'04, 2004, pp. 78–87.

[8] S. Meguerdichian, F. Koushanfar, M. PotKonjak, M.B. Srivastava, Coverage problems in wireless ad-hoc sensor networks, in: Proceedings of IEEE Infcom, vol. 3, Anchorage, Ak, 2001, pp. 1380–1387.

[9] S. Meguerdichian, F. Koushanfar, M. PotKonjak, M.B. Srivastava, Worst and best-case coverage in sensor networks, in: IEEE Transactions On Mobile Computing, vol. 4, 2005, pp. 84–92.

[10] X. Li, Peng-JunWan, O. Frieder, Coverage in wireless ad hoc sensor networks, IEEE Transactions on Computers 52 (6) (2003) 753–763.

[11] D. Mehta, M. Lopez, L. Lino, Optimal coverage paths in ad-hoc sensor networks, in: IEEE International Conference on Communications, vol. 1, 2003, pp. 507–511.

[12] J. Liu, X. Koutsoukos, J. Reich, F. Zhao, Sensing field: coverage characterization in distributed sensor networks, in: IEEE ICASSP, vol. 5, 2003, pp. 173–176.

[13] G. Kesidis, T. Konstantopoulos, S. Phoha, Surveillance coverage of sensor networks under a random mobility strategy, in: Proceedings of IEEE Sensors, vol. 2, 2003, pp. 961–965.

[14] K. Chakrabarty, S.S. Iyengar, H. Qi, E. Cho, Grid coverage for surveillance and target location in distributed sensor networks, IEEE Transactions On Computers 51 (12) (2002) 1448–1453.

[15] K. Chakrabaty, S. Iyengar, Sensor placement in distributed sensor networks using a coding theory, Framework (2001) 157.

[16] R. Kannan, S. Sarangi, S. Ray, S.S. Iyengar, Minimal sensor integrity: measuring the vulnerability of sensor deployments, Information Processing Letters 86 (1) (2003) 49–55.

[17] L. Benyuan, D. Towsley, On the coverage and detectability of large-scale wireless sensor networks, 2003.

[18] Y. Zou, K. Chakrabaty, Uncertainty-aware and coverage-oriented deployment for sensor networks, Journal of Parallel and Distributed Computing 64 (7) (2004) 788–798.

[19] S. Meguerdichian, S. Slijepcevic, V. Karayan, M. Potkonjak, Localized algorithms in wireless ad-hoc networks: Location discovery and sensor exposure, in: Proceedings of 2001 ACM International Symposium. Mobile Ad Hoc Netw. Comp. MobiHoc, 2001 pp. 106–116.

[20] S. Meguerdichian, F. Koushanfar, G. Qu, M. Potkonjak, Exposure in wireless ad hoc sensor networks, in: Proceedings of the Annual International Conference on Mobile Computing and Networking, Rome, 2001, pp. 139–150.

[21] A. Tews, M.J. Mataric, G. Sukhatme, Avoiding detection in a dynamic environment, in: IEEE RSJ International Conference on Intelligent Robots and Systems 4, 2004, pp. 3773–3778.

[22] A. Howard, J.J. Matarić, G.S. Sukhatme, An incremental self-deployment algorithm for mobile sensor networks, Autonomous Robots, Intelligent Embedded Systems 13 (2) (2002) 113–126 (special issue).

[23] A. Kansal, M. Rahimi, D. Estrin, W.J. Kaiser, G.J. Pottie, S.M.B, Controlled mobility for sustainable wireless sensor networks, in: First Annual IEEE Communcations Society Conference Sensor Ad Hoc Communcation Networks. IEEE SECON, 2004 pp. 1–6.

[24] S. Ganeriwal, A. Kansal, M. Srivastava, in: IEEE Proceedings of International Conference on Robotics and Automation, pp. 5244–5249.

[25] M. Rahimi, H. Shah, G.S. Sukhatme, J. Heideman, D. Estrin, Studying the feasibility of energy harvesting in a mobile sensor network, in: Proceedings of IEEE International Conference on Robotics and Automation, vol. 1, Taipei, Taiwan, 2003, pp. 19–24.

[26] S. Čapkun, J.-P. Hubaux, L. Buttyàn, Mobility helps security in ad hoc networks, in: Proceedings of ACM International Symposium on Mobile Ad Hoc Network and Computing, Annapolis, Maryland, 2003, pp. 46–56.

[27] M. Laibowitz, J. Paradiso, Parasitic mobility in dynamically distributed sensor networks, Pervasive Computing: Third International Conference 3468 (2005) 255–278.

[28] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing,MobiHoc'05, Urbana-Champaign, IL, 2005, pp. 46–57.

[29] K. Ma, Y. Zhang, W. Trappe, Mobile network management and robust spatial retreats via network dynamics, IEEE MASS 2005 Workshop - RPMSN05.

[30] A. Wood, J. Stakovic, S. Son, Jam: a jammed-area mapping service for sensor networks, IEEE International Real-Time Systems Symposium RTSS (2003) 286–297.

[31] T. Camp, J. Boleng, V. Davies, A survey of mobility models for ad hoc network research, Wireless Communication & Mobile Computing (WCMS): Mobile Ad Hoc Networking: Research, Trends and Applications 2 (5) (2002) 483–502 (special issue).

Alexandra Czarlinska is a Ph.D. candidate in the Wireless Communications Group (WCL) in the Department of Electrical & Computer Engineering at Texas A& M University under the supervision of Dr. Deepa Kundur. She received her B.A.Sc. degree in Engineering Science (Electrical Option) in 2002 from the University of Toronto Canada where she was the recipient of the National Scholarship Award. Her current research focuses on the identification and prevention of new security attacks in mobile wireless sensor and actuator networks.

Deepa Kundur received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in electrical & computer engineering in 1993, 1995, and 1999, respectively, from the University of Toronto, Canada. In January 2003, she joined the Department of Electrical & Computer Engineering at Texas A&M University where she is an Associate Professor and leads the SeMANTIC (Sensor Media Algorithms & Networking for Trusted Intelligent Computing) Research Group of the Wireless Communications Laboratory. Her research interests include security and privacy for scalar and broadband sensor networks, multimedia security, digital rights management, steganalysis for computer forensics, and dynamical systems theory. She has given tutorials in the area of information security at ICME-2003 and Globecom-2003, and was a Guest Editor of the June 2004 Proceedings of the IEEE Special Issue on Enabling Security Technologies for Digital Rights Management and the EURASIP Journal on Advances in Signal Processing Special Issue on Visual Sensor networks. She currently serves as the Vice-Chair for the Security Interest Group of the IEEE Multimedia Communications Technical Committee and is an Associate Editor for the IEEE Communication Letters and IEEE Transactions on Multimedia.